

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

FINJAN SOFTWARE, LTD., an Israel corporation,)	
)	
Plaintiff,)	Civil Action No. 06-369 GMS
)	
v.)	
)	
SECURE COMPUTING CORPORATION,)	
a Delaware corporation, CYBERGUARD,)	
CORPORATION, a Delaware corporation,)	
WEBWASHER AG, a German corporation and)	
DOES 1 THROUGH 100,)	
)	
Defendants.)	

**DECLARATION OF JAMES HANNAH IN SUPPORT OF
PLAINTIFF FINJAN SOFTWARE, LTD.'S REPLY BRIEF
IN SUPPORT OF ITS COMBINED MOTIONS FOR ENHANCED
DAMAGES AND ATTORNEYS' FEES, EXPENSES AND COSTS**

OF COUNSEL:

Paul J. Andre
Lisa Kobialka
KING & SPALDING LLP
1000 Bridge Parkway
Suite 1000
Redwood City, CA 94065
(650) 590-0700

Philip A. Rovner (#3215)
POTTER ANDERSON & CORROON LLP
Hercules Plaza
P. O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com

Attorneys for Plaintiff
Finjan Software, Ltd.

Dated: May 16, 2008

I, JAMES HANNAH, declare:

1. I am an attorney with the law firm King & Spalding LLP, counsel of record for Plaintiff Finjan Software, Ltd. ("Finjan"). I have personal knowledge of the facts set forth in this declaration and can testify competently to those facts.

2. Attached hereto as Exhibit 1 is a true and correct copy of Trial Exhibit PTX-16, an email from Christoph Alme to Martin Stecher dated May 28, 2004.

3. Attached hereto as Exhibit 2 is a true and correct copy of Trial Exhibit PTX-37, Secure Computing Product Meeting Minutes dated June 29, 2004.

4. Attached hereto as Exhibit 3 is a true and correct copy of Trial Exhibit PTX-42, a Secure Computing white paper entitled "Overcoming addition to signatures."

5. Attached hereto as Exhibit 4 is a true and correct copy of the Conference Call Transcript of the SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call on May 1, 2008.

6. Attached hereto as Exhibit 5 is a true and correct copy of pages from Trial Exhibit JTX-14, a Finjan manual entitled "Vital Security for Web 7.0 User Manual," dated 2004.

7. Attached hereto as Exhibit 6 is a true and correct copy of pages from Trial Exhibit DTX-1070, a Finjan manual entitled "Management Console Reference Guide - Vital Security Web Appliances NG-1100/NG-5100/NG/8100," dated 2006.

8. Attached hereto as Exhibit 7 is a true and correct copy of an email from Lisa Kobialka, counsel for Finjan, to Jake Holdreith, counsel for Secure Computing, dated February 27, 2008.

9. Attached hereto as Exhibit 8 is a true and correct copy of an email from Kris Kastens, counsel for Finjan, to Christopher Seidl, counsel for Secure Computing, dated November 30, 2007.

10. Attached hereto as Exhibit 9 is a true and correct copy of a letter from Christopher Seidl to me dated September 28, 2007, enclosing an Affidavit of Paul Judge.

11. Attached hereto as Exhibit 10 is a true and correct copy of the Secure Computing Company Fact Sheet, *available at*
<http://www.securecomputing.com/index.cfm?skey=233&menu=about>.

I declare under penalty of perjury under the laws of the State of California and the United States of America that each of the above statements is true and correct.

Executed in Redwood City, California on May 16, 2008.

By: _____


James Hannah

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

CERTIFICATE OF SERVICE

I, Philip A. Rovner, hereby certify that on May 16, 2008, the within document was filed with the Clerk of the Court using CM/ECF which will send notification of such filing(s) to the following; that the document was served on the following counsel as indicated; and that the document is available for viewing and downloading from CM/ECF.

BY HAND DELIVERY AND E-MAIL

Frederick L. Cottrell, III, Esq.
Kelly E. Farnan, Esq.
Richards, Layton & Finger, P.A.
One Rodney Square
920 N. King Street
Wilmington, DE 19801
cottrell@rlf.com; farman@rlf.com

I hereby certify that on May 16, 2008 I have sent by E-mail the foregoing document to the following non-registered participants:

Jake M. Holdreith, Esq.
Christopher A. Seidl, Esq.
Robins, Kaplan, Miller & Ciresi L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
jmholdreith@rkmc.com; caseidl@rkmc.com

/s/ Philip A. Rovner
Philip A. Rovner (#3215)
Potter Anderson & Corroon LLP
Hercules Plaza
P.O. Box 951
Wilmington, Delaware 19899
(302) 984-6000
E-mail: provner@potteranderson.com

Exhibit 1

From: Christoph Alme
To: Martin Stecher
CC: Jan Schnellbacher; Peter Borgolte; Frank Berzau; Benita Sieben-Ostmann
BCC:
Sent Date: 2004-05-28 15:05:43:000
Received Date: 2004-05-28 15:05:43:000
Subject: RE: Proactive Security
Attachments:

Within the Proactive Security feature (a.k.a. the "injan Killer") we found basically two fundamentally different approaches. Please have a look which of these does better meet corporate policy and sales desire.

We will need to write a scanner for JavaScripts, VB-Scripts, Java Applets, ActiveX Controls and other binaries.

>>> Ein weiterer Parser für VBA wäre zwar evtl. etwas schwieriger zu implementieren als für BScript, würde aber zumindest ein Alleinstellungsmerkmal gegenüber Finjan darstellen, die ja Officedokumente gar nicht prüfen.

After the scan, WW must decide what to do with the file. Then we can do one of these options:

1. Look for potentially dangerous stuff within those files. The problem here is that the scanner can only check for some few criteria and there will be tons of bypass vulnerabilities; especially in binary code (such as in ActiveX controls) calls to dangerous functions can easily be overseen by the scanner.

2. Only allow those files for which a scanner can determine that it is harmless. This would only be a minority of files as scanning of for example Active X binaries is limited and the code would need to reject all files that call any unknown kernel function. For JavaScripts we could implement a parser that would execute some hard to parse function calls in a sandbox to verify the parameters making this.

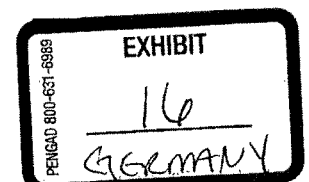
>>> Vielleicht noch wichtig zu betonen, das IR definieren, was wir unter "harmless" verstehen, u. der Admin es nicht selbst konfigurieren kann/soll (im GgStz. zu Finjan, bzw. nicht so granular) ? Also z.B. alle Skripte, die keines der Kriterien

- Skript nutzt ActiveX Controls
- Skript generiert Code dynamisch (= eval() in JavaScript/Execute() in BScript)
- =..

Plaintiff's Trial Exhibit

PTX-16

Case No. 06-369 GMS



erfüllen, sind harmlos. Alle anderen, die eines der obigen Kriterien erfüllen, werden geblockt, der Anwender erhält mit der Blockmeldung eine TicketID usw.

Option 1 is what Finjan does. Question is whether our (new) corporate policy allows us to follow this path. It pretends some deep level of security, which is actually not there. We would not feel comfortable with promoting this approach. On the other hand it is that what Finjan has and we would compete exactly with them. But it will also give us a hard time as we cannot expect that the first version will have the same number of filter settings and capabilities. They will also check very carefully which of their patents we may touch by recreating their system.

Option 2 contains something like a real sandbox for JavaScript, which even Finjan does not have. On the other hand this technology may corrupt some web pages and may create many false positives, especially for the binary files, which the scanner cannot easily parse, more than 90% of the files would not be considered harmless.

This would be the strategy of all customers that like to have a tight Internet policy but do not want to block everything, especially in the JavaScript context but could afford to block nearly all executables. In order to make it feasible we should add a fingerprint database in form of a subscription model that will allow us to continuously update a white list of files that we found to be harmless in our lab but would be detected as not harmless by the scanner. An automatic feedback function would allow the customer to send classified files to us for further investigations. This costs many additional resources in TPT.

Whatever option we choose or whether you wish to suggest an alternative way, this feature will cost a lot of resources. Surprise, surprise that a feature that Finjan works on for years cannot be done within a few weeks.

Exhibit 2

From:
To:
CC:
BCC:
Sent Date: 0001-01-01 00:00:00:000
Received Date: 0001-01-01 00:00:00:000
Subject:
Attachments:

FYI

----- Original Message -----

Subject: Product Meeting minutes June 29, 2004
Date: Thu, 1 Jul 2004 17:30:00 +0200
From: Frank Berzau <frank@WEBWASHER.com>
To: Thomas Friedrich <thomas.friedrich@WEBWASHER.com>, Heiko Giesselmann <heiko.giesselmann@WEBWASHER.com>, Peter Borgolte <peter.borgolte@WEBWASHER.com>, Benita Sieben-Ostmann <benita.sieben@WEBWASHER.com>, Martin Stecher <martin.stecher@WEBWASHER.com>, Bart-Jan Schuman <bart-jan.schuman@WEBWASHER.com>, Tom Bryant <tom.bryant@WEBWASHER.com>, Horst Joepen <horst.joepen@WEBWASHER.com>, Christian Matzen <christian.matzen@WEBWASHER.com>, Jobst Heinemann <jobst.heinemann@WEBWASHER.com>, Gary Taggart <gary.taggart@WEBWASHER.com>

Participants: Peter, Roland, Benita, Heiko, Tom

1. State of Kentucky issues
2. CR status
3. WW status
4. Akonix

1) state of kentucky, Tom reports an issue with a lib with av, Tom to forward to Benita while Marek is on vacation

2) Maxdb integration making progress, db space mgmt missing
Feature discussion last week, no hot customer issues
4.3 targeted end of quarter, but will be later (maybe 10 days from today)

3) This week bugfix release with special feature for unicode handling
5.1 planning: Christoph and Jan started research proactive security features, also Roland doing research on proact. sec patents from finjan and trend

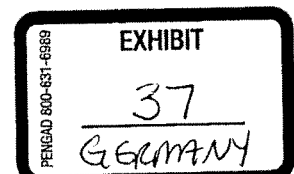
Urgent need for someone who does documentation. Cognitas (outsourcing docs) we will get a very good resource for three months, potential to extend.

Appliance: Frank will take CD to the sales meeting so we can demo

Plaintiff's Trial Exhibit

PTX-37

Case No. 06-369 GMS



Spyware paper from Roland will be published on website today or tomorrow

4) Tom reports protocol updates with akonix failing

Exhibit 3

SECURE
COMPUTING

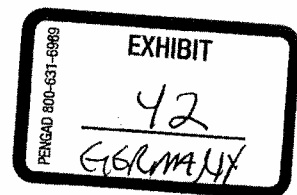
Overcoming addiction to signatures.

Oliver Braekow
Product Marketing Manager
© 2006, Secure Computing

Plaintiff's Trial Exhibit

PTX-42

Case No. 06-369 GMS



1/12



Index

Index	2
Introduction	3
State of the "virus union"	4
Comparison of anti-virus response times	5
Reaction times to Sober.C in 2003	5
Reaction times to Zotob/A Worm in 2004	5
Reaction times to Nyxem Worm in 2006	6
Conclusion	6
Why signature based anti-virus can't keep up	7
Fresh approaches to solve the problem	8
General considerations	8
Considerations for the client	8
Considerations for the gateway	9
Fighting malware without signature updates	10
Verdict	10
Webwasher Anti-Malware	11
Sources and references	12



Introduction

You might think: "I have an Anti-Virus solution from one of the leading vendors installed on every PC and server and I even have an anti-virus proxy on my gateways, checking all incoming e-mail messages and all Web traffic for Viruses, so I must be ok"

Well certainly this gives a certain degree of "piece of mind" and even might suffice to tick the checkbox for your compliance questionnaire, but do you really feel safe with this? Certainly a lot of people don't.

According to the 2006 CSI/FBI Computer and Crime survey [1] virus protection is still critical item ranked #4 when it comes to IT, only surpassed by data theft (which somewhat ties into this problem as we will see later), compliance and policy regulations.

And it is so for a good reason: Albeit 97% of the enterprises surveyed use anti-virus software and 98% even used a firewall, almost two third (65%) suffered a Virus outbreak or incident.

313 organizations of the survey specified the combined cost of losses due to virus outbreaks and bots (zombies) within the organization at \$16.6 Million, or an average of > \$50k a company, despite having an anti-virus solution on place.

This whitepaper will discuss some of the causes for this waste of money and show new and potentially more cost effective solutions.

State of the "virus union"

This document will use the term malware synonymous for everything that someone might consider a virus, spyware, trojan, rootkits, bots, hijackers, ransom-ware - generally for every form of active content that most IT administrators don't want to have in their network.

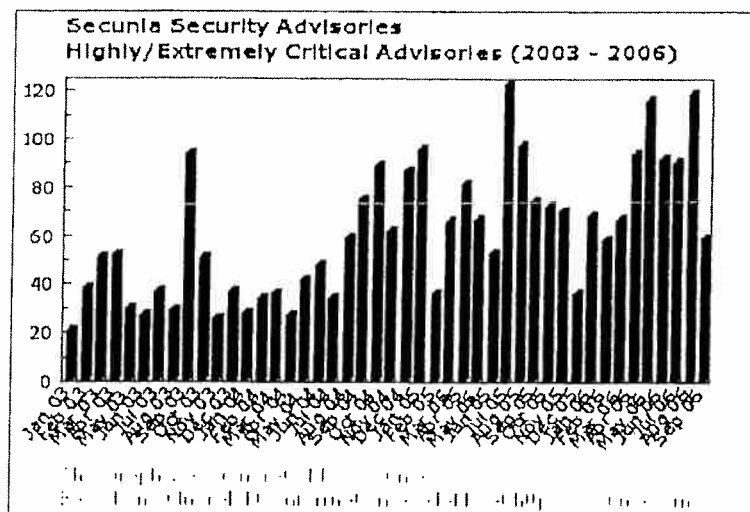
We will not cover "static" Media types that are unwanted like Streaming videos, pictures/graphics etc.

Ten years ago, when nearly all of today available Anti-Malware solutions were architected the typical piece of Malware was written by a nerd computer kid or a dissatisfied employee. Its sole purpose was to wreak havoc, cause harm and increase the self esteem and prestige of the writer. Only few individuals had the time and the skills to create a piece of Malware, and even fewer the skills to make it self-propelled.

So Ten years ago it was a comfortable and sound approach to create a snapshot, (sometimes also called signature) of that piece of Malware and to identify with simple lookup mechanism.

Those were the good old times.

Today most everybody that is somewhat IT savvy and connected to the Internet can create a piece of Malware. There are resources all over the Internet ([2][3][4][5]) to educate, sometimes even download toolkits to create Malware. Sometimes those sites are meant to enhance the security awareness, but ill fated individuals will find it easy to convert these sources to be used for malicious purposes. So more and more individuals are actually skilled to create a piece of Malware, and it is even easier to find an access point. According to Secunia [6] the number of vulnerabilities is constantly on the rise, on average quadrupling from February 2003 to August 2006.



Picture 1 : Historical Secunia advisories [6]

So there is more and more individuals' capable of creating some form of malware and malware is available for download and there are more and more targets for this newly created malware. Where does this leave us?

The number of actual malware appearances has grown exponentially over the last few years. On July 6th 2006 McAfee issued a press release that it had taken them almost 18 years to populate their database with the first 100,000 malicious samples, but just under to years to grow to 200,000 samples and that they expect to reach 400,000 threats within the next two years [7].

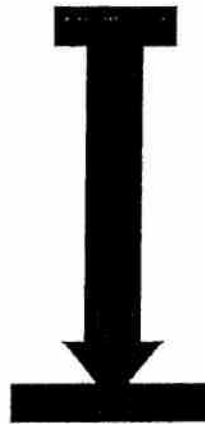
Traditional anti-virus vendors react to this flood of malware by upgrading their systems so they now have not only a few dozen but hundreds or even thousands of sources and streamlining their processes, so a new piece of malware can be investigated and transformed into a signature within a few hours. But did this help?

Comparison of anti-virus response times.

Anti-virus companies have been doing a seemingly good job becoming more efficient, upgrading their systems and getting out patches and signature updates automatically to cope with the load of new malware appearing. Yet we've seen that almost two third of enterprises had a virus incident in 2005. To understand this let's have a look at some real world examples of reaction times to very some well known aggressive worms and viruses:

Reaction times to Sober.C in 2003

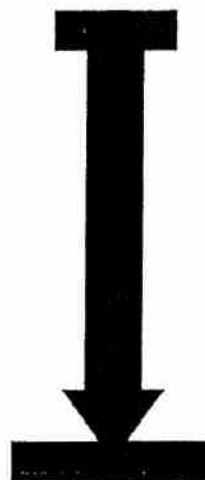
WORM discovered	2003-12-20 03:00
BitDefender	2003-12-20 13:20
Kaspersky	2003-12-20 14:44
F-Prot(Frisk)	2003-12-20 15:25
F-Secure	2003-12-20 15:45
Norman	2003-12-20 18:25
eSafe(Aladdin)	2003-12-20 18:35
TrendMicro	2003-12-20 19:50
AVG(Grisoft)	2003-12-20 20:15
AntiVir(H+BEDV)	2003-12-20 22:20
Symantec	2003-12-21 04:05
Avast!(Alwil)	2003-12-21 09:55
Sophos	2003-12-21 14:35
Panda AV	2003-12-21 17:05
McAfee	2003-12-22 04:10
Ikarus	2003-12-22 10:35
eTrust(CA)	2003-12-22 17:50
AVG (GData)	2003-12-23 23:50



Picture 2 : Response times to W32/Sober.C / Source: AV-test.org [8]

Reaction times to Zotob/A Worm in 2004

Webwasher	Blocked w/o update
Kaspersky	2005-08-16 21:57
QuickHeal	2005-08-16 22:48
ClamAV	2005-08-16 23:12
eTrust-INO	2005-08-16 23:51
F-Secure	2005-08-17 00:03
AntiVir	2005-08-17 00:19
Sophos	2005-08-17 00:44
Trend Micro	2005-08-17 00:44
McAfee	2005-08-17 01:34
eTrust-VET	2005-08-17 01:53
Symantec	2005-08-17 03:05
Command	2005-08-17 03:40
Dr Web	2005-08-17 07:04
Ikarus	2005-08-17 07:41
Avast	2005-08-17 08:04
AVG	2005-08-17 11:33
Hauri	2005-08-17 13:45
VirusBuster	2005-08-17 14:32
Proland	2005-08-18 11:16



Picture 3: Reaction times of AV vendors to first Zotob Worm[9]

Reaction times to Nyxem Worm in 2006

Webwasher	Blocked w/o update (ProActive)
McAfee	Blocked w/o update (Heuristics)
QuickHeal	16.01.2006 10:00
Bitdefender	16.01.2006 12:13
Kaspersky	16.01.2006 13:44
AntiVir	16.01.2006 14:52
Karus	16.01.2006 15:27
Dr Web	16.01.2006 15:56
F-Secure	16.01.2006 16:03
F-Prot	16.01.2006 16:31
Command AV	16.01.2006 17:04
AVG	16.01.2006 17:05
Sophos	16.01.2006 17:25
Ewido	16.01.2006 19:08
Trend Micro	17.01.2006 04:16
Trust-VET	17.01.2006 07:39
Norman	17.01.2006 08:49
ClamAV	17.01.2006 09:47
Avast!	17.01.2006 16:31
eTrust-INO	17.01.2006 17:52
Symantec	17.01.2006 18:03



Picture 4 : Reaction times of AV vendors to Nyxem worm [10]

Conclusion

Traditional Anti-Virus solutions are hardly keeping up. The reaction times of popular anti-virus engines didn't improve at all since 2003. Even worse, the "big three" providers sharing almost 90% of the anti-virus market didn't show improvement at all, but are rather getting slower reacting to new malware.

Why signature based anti-virus can't keep up

- a) **Malware attacks are much more focused:** Gone are the old shotgun herd attacks. Today's malware is focused on users with specific behavior patterns. It largely depends on what the user does, what sites he accesses online, whether he downloads material from risky sites, and how careful he/she is about downloading files attached to e-mails, and similar issues. The traditional one solution fits all approach is no longer applicable.
- b) **Malware changes its code constantly:** There are viruses out there automatically changing (morphing) every single day and every time they send themselves out. Anti-virus vendors either have to use performance hungry heuristics or have a really hard time keeping up
- c) **Malware means money:** Malware is no longer a preteen prank. It is organized crime. The perpetrators either are or employ talented software engineers who are as good as those in anti-malware companies, and they stay at least one step ahead of the good guys. More often malware is actually used for corporate espionage, as the infiltration of the Israel HOT cable television group network in 2005 showed [11].
- d) **Some malware remover is actually malware:** This is a deceitful trap for users. Some XXX websites are rumored to have deals in place with malware authors. E.g. when someone accesses the site he gets a fake error message that his/her system is penetrated and is urged to click a link and download a "test utility" to scan. This test utility is usually a piece of spyware in a seemingly benign system cleaner wrapper or similar.
- e) **Standard antivirus programs are often ineffective:** The malware designers constantly test their creations against Norton, McAfee, and other popular anti-virus and anti-spyware systems, so they know those programs will not detect the malware when it goes out. By the time the good guys catch up, the damage is done, and the bad guys change their code to make it undetectable again. Sometimes these code changes are even automatic (morphing, see above).
- f) **Hide and seek:** More and more malware actually tries to hide itself by using rootkit mechanisms or completely disabling anti-virus software on the client in the first place [12].



Fresh approaches to solve the problem

General considerations

Don't rely on a pure client or pure gateway solution. If you have a client side anti-virus subscription - great the first step is done, but add an anti-malware solution for your gateway.

Important: All application protocols entering your network need to be under close scrutiny. Most everybody today has some form of anti-spam and anti-virus combination - but what about your web gateway? It is as important as your mail gateway. Even for more exotic protocols like HTTPS or instant messaging: Either you control it or you close it. There is various tools out there to enable control over HTTPS traffic, such as the Webwasher SSL Scanner [13].

Even for the most exotic Instant Messaging application: You can control or at least stop it. Secure Computing IM Filter allows blocking of unsanctioned usage of Instant Messaging and Peer-Peer applications such as Skype or Kazaa. If you want to allow Instant Messaging - and control it - consider the Secure Computing IronIM solution [14].

Considerations for the client

Analyzing the VirusBulletin malware prevalence table for 2006 [15], none of the top 30 pieces of malware reported this year is spreading via manual/physical distribution. All are actually self-propelled and use Mail, Instant messaging or Network shares to spread. Knowing this it is safe to say virus-scanning at the client is actually getting less important, while file servers and gateways on the switch side need much more focus.

One of the main reasons for this: the typical boot sector virus that used to reside on a floppy is extinct - because there are no more floppy drives. The only issue someone might worry about is the usage of USB memory devices or viruses on a CD, so there is some form of necessity for anti-virus at the client, however don't spend all your money on this one.

The typical worm, virus or piece of spyware today only replicates via e-mail or via the network, if you encounter a different one it is either:

- fairly old and even the worst anti-virus engine has a signature for it, or
- a targeted attack at your company or your domain and it is unlikely even the most expensive anti-virus solution has a signature for it.

So don't put your focus here. Consider a conveniently priced anti-virus with good Integration Into Windows, even Microsoft OneCare [16] or the free open source ClamAV [17] will do the job.

If you feel you need additional protection at the client consider the use of application control and endpoint control solutions as provided by SecureWave [18] or Appsense [19] or others. These solutions actually work with the positive security model allowing only allow "known good processes" on your client machine or server and block any "not allowed" applications or scripts from starting. The downside of this is obviously the loss of control over the PC for the individual end user, but often that is a highly desired side effect.

Considerations for the gateway

As we've seen above the importance of malware scanning of all open protocols at the gateway has become increasingly important to keep your network free of malware or other potentially unwanted programs (PUPs).

Almost all anti-virus vendors offer a gateway solution of their offerings, so customers have a great variety of solutions to choose from. Traditional signature only based solutions however face the same limitations as on the client, so consider the following when selecting a gateway security solution:

Avoid monoculture: Having the same solution on the client and at the gateway is an inexcusable faux-pas. Especially if the solution is entirely signature based the chance of a new piece of malware entering undetected through the gateway and not being discovered at the client makes this an inexcusable mistake. Most anti-virus vendors try to lure their corporate customers with a bundled pricing for unlimited gateway use if they buy the client solution or vice versa. Don't fall for this bait. Differentiate or accept having a virus incident.

Cover all open protocols: Everybody knows it is easy to check for malware in mails and web traffic – but malware can spread as easily via peer-peer, instant messaging and encrypted https connections. There are easy to deploy solutions to extend the reach of anti-malware to HTTPS [13] and IM traffic [14] on top of existing solutions. Consider deploying these or blocking these protocols entirely.

Don't rely on a single anti-malware solution: the odds of one anti-malware vendor always being the first one to reliably stop new attacks are pretty low. Consider deploying more than one solution for your gateway. Hardware is cheap and some vendors offer bundles of anti-malware / anti-virus engines - put this to good use.

Reduce your dependency on signatures: Above we learned that traditional anti-virus vendors can hardly keep up with new forms and variations of the malware flood. There are additional ways to tackle the malware problem and not relying entirely on timely signature updates. These are discussed below.

Fighting malware without signature updates

Heuristics: some traditional anti-virus solutions introduce so called "heuristics" to find slight variations of signatures. Tests have shown this is not going to solve the problem, as the typical detection rate doesn't improve significantly [20]. It gives some relief, but it can't be considered a final solution. Adding heuristics has negative impacts on performance and false positives. Refer to the "Proactive Security step-by-step guide" [20] for details on why heuristics can't match real behavior based solutions.

Sandboxing: Other solutions include "sandboxing" [21], describing a method to create a virtual encapsulated environment to determine the potentially malicious behavior of a piece of active code. Sandboxing at the gateway is mostly prohibitive because of performance bottlenecks for setting up an executable sandbox environment and because the gateway usually has no way of reliably finding out how to emulate the environment the executable code needs to run in correctly.

Proactive behavioral analysis: real proactive solutions are – at least partially- based on behavioral analysis and blocking of suspicious code. Proactive security filters iterate potential function calls regardless of the actual program flow of the active code. Known functions are classified based on a given set of rules. Depending on the program code language, detected function calls are put into relation and again compared against a given set of context-sensitive rules. A more detailed description is available of the proactive filters in Secure Computing Anti-Malware is given in [22].

Reputation based connection control: This term refers to controlling where employees go to when surfing the web (URL-Filter) or checking incoming e-mails for known "bad senders" one cannot expect good or wanted traffic from (Connection Control). While this technique is a brilliant way to enhance solutions in place, it doesn't provide the level of security that one can solely depend on. There will always be websites or sender IP's for mails that are not categorized and that need some form of additional treatment before the final verdict of good/bad can be done. Claims by companies to provide a big and "up to date" enough database to be able to judge if a URL or a sender IP is "malicious" should be questioned carefully. This would be the same as constantly and in real time monitoring each website and each IP address on the internet. Given the rate at which new websites and web servers appear and disappear this will lead to the same "late signatures" problem as with traditional anti-malware solutions.

Verdict

Companies today have and will need anti-malware solutions for the client. Given the self propelled nature of malware today, gateway based solutions come to focus. To keep up with the growing flood and sophistication of malware, signature based solutions need to be augmented by smarter "proactive" solutions and should even be combined with some form of connection control (URL-Filter, E-Mail blocking based on reputation of sender) to prevent being bombarded with malware in the first place. Pathways (protocols) that are not under control now (https, IM) but needed for business relevant purposes need to be put under control, others should be closed, as new forms of malware otherwise find their way into the organization.

The Webwasher Anti-Malware product by Secure Computing represents one of the few solutions available on the market today fulfilling all these requirements.

Webwasher Anti-Malware

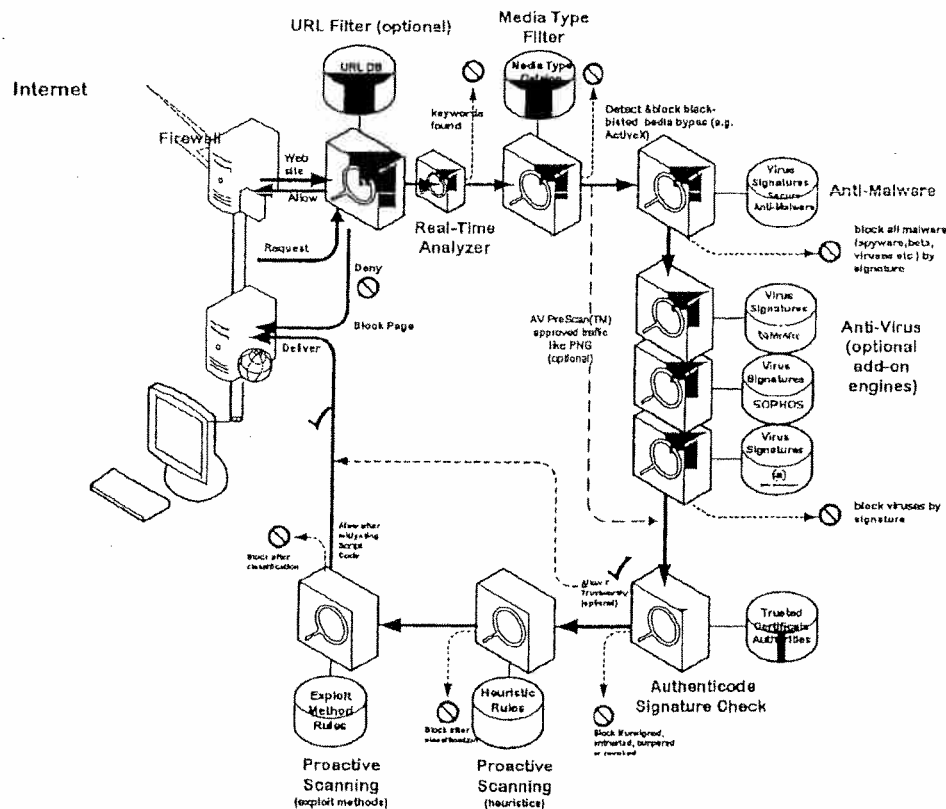
Webwasher Anti-Malware by Secure Computing is a gateway product inspecting all incoming and outgoing code in up to five steps. As a first step, magic byte inspection of each file determines the corresponding correct media type. Corporations may want to disallow media types that are potentially hazardous (like ActiveX), bandwidth intensive or drain productivity, e.g. video streams.

As a next step the *Secure Anti-Malware* engine inspects the traffic for known bad signatures of viruses, spyware, bots or other potentially unwanted programs. To improve performance, files of certain types without known signatures in the engine (e.g. .png) can bypass the signature based anti-virus engine safely. This technology, PreScan™, frees up enough bandwidth to enable the following deep inspection mechanisms without performance penalty.

In the next step all active code is examined for digital signatures. Administrators have very granular settings to allow, block or inspect active code based on the issuer or signature validity.

As the next step, a heuristic analysis is performed, where potential function calls are iterated regardless of the actual program flow and known functions are classified based on a given set of rules. Depending on the program code language, detected function calls are put into relation and again compared against a given set of context-sensitive rules.

In a fifth and final step scripts trying to exploit vulnerabilities on the client are scanned and neutralized. Although the scripts are not malicious per se, they are the enablers to inject or execute further malicious code. Detecting and neutralizing such scripts on the gateway interrupts the malicious payload of being distributed to the clients. A comprehensive set of methodologies scans and analyzes the scripts versus an automatically updated database of rules. Known or unknown script code utilizing exploits is reliably detected by probability weightings.



Picture 5 : Anti-Malware approach to gateway security



Sources and references

- [1] Computer Security Institute: <http://qocsi.com/> 2006 CS/IFBI COMPUTER CRIME AND SECURITY SURVEY
- [2] <http://www.astalavista.net/>
- [3] <http://www.metasploit.org/>
- [4] <http://astalavista.box.sk>
- [5] <http://www.blackcode.com/>
- [6] http://secunia.com/graph/?type=all&graph=adv_om
- [7] McAfee Inc. Press release, July 6th 2006:
<http://phx.corporate-ir.net/phoenix.zhtml?c=104920&p=irol-newsArticle&ID=879176&highlight=>
- [8] <http://www.av-test.org/index.php3?lang=en>
- [9] Source: <http://www.pcwelt.de/news/sicherheit/118264/index2.html>, data by AV-Test.org
- [10] Source: <http://www.pcwelt.de/news/sicherheit/130720/index2.html>, data by AV-Test.org
- [11] Computerworld Security (online): Israel holds couple in corporate espionage case Trojan writers helped top corporations spy on each other.
http://www.computerworld.com/securitytopics/security/virus/story/0,10801,108225,00.html?from=story_kc
- [12] <http://en.wikipedia.org/wiki/Rootkits>
- [13] Secure Computing Webwasher SSL Scanner: <http://www.securecomputing.com/index.cfm?skey=1536>
- [14] Secure Computing IronIM appliance: <http://www.ciphertrust.com/products/ironim/>
- [15] Malware prevalence for 2006, VirusBulletin
<http://www.virusbt.com/resources/malwareDirectory/prevalence/index.xml?year=2006>
- [16] <http://www.windowsoncare.com/>
- [17] <http://www.clamav.net/>
- [18] SecureWave website: <http://www.securewave.com>
- [19] Appsense website: <http://www.appsense.com>
- [20] "Proactive Security Step-by-step guide" available from the Secure Computing resource center
http://www.securecomputing.com/resourcecenter_main.cfm
- [21] Wikipedia sandboxing description http://en.wikipedia.org/wiki/Sandbox_%28security%29
- [22] Secure Computing SCM products overview: <http://www.securecomputing.com/index.cfm?skey=1486>

Exhibit 4

FINAL TRANSCRIPT



Conference Call Transcript

SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Event Date/Time: May. 01. 2008 / 4:30PM ET

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

CORPORATE PARTICIPANTS

Jane Underwood

Secure Computing Corporation - IR

Tim Steinkopf

Secure Computing Corporation - SVP of Operations & CFO

Dan Ryan

Secure Computing Corporation - CEO

CONFERENCE CALL PARTICIPANTS

Eric Martinuzzi

Craig-Hallum Capital Group - Analyst

Rob Owens

Pacific Crest Securities - Analyst

Jonathan Ruykhaver

ThinkEquity Partners - Analyst

Fred Ziegel

Soleil Securities - Analyst

Josh Jabs

Roth Capital Partners - Analyst

Fred Green

Goldman Sachs - Analyst

Joe Maxa

Dougherty & Company - Analyst

Katherine Egbert

Jefferies & Company - Analyst

Eric Suppiger

Signal Hill Group LLC - Analyst

Todd Raker

Deutsche Bank - Analyst

Joel Fishbein

Lazard Capital Markets - Analyst

PRESENTATION

Operator

Welcome to Secure Computing Corporation's first quarter 2008 results conference call. All participants will be able to listen only until the question and answer session, which will follow today's presentation. (OPERATOR INSTRUCTIONS) Today's call is being recorded. If there are any objections, please disconnect at this time. I will now turn the call over to Miss Jane Underwood, Vice President for Investor Relations.

Jane Underwood - *Secure Computing Corporation - IR*

Good afternoon. And thanks for joining us to discuss our first quarter results. On the call with me today with Dan Ryan, our CEO; and Tim Steinkopf, our Senior Vice President of Operations and CFO.

Before I turn the call to Tim, I'm going to make a cautionary statement regarding forward-looking statements. During the course of this call and the question and answer session following management's remarks, we will make forward-looking statements that involve risks and uncertainties.

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Such forward-looking statements are subject to the Safe Harbor created by the Private Securities Litigation Reform Act of 1995. These statements include, for example, statements regarding future results such as guidance for second quarter billings, revenue, gross margin, operating expense, tax expense, interest and other expense, expense reductions, shares outstanding, earnings per share and cash flows and cash balances and statements about our sales pipeline, the breakdown of sales across our product lines and success and availability of our products. Our actual results could differ materially from the forward-looking statements. Factors which could cause actual results to differ include for example risks related to the competition in the securities industry, changes in customer requirements, delays in product development, and the other factors and risks identified in our press release and our SEC filings. We do not undertake any obligation to correct or update any forward-looking statements that may become inaccurate. Now, I would like to turn the call over to Tim.

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

Thank you, Jane. Since our final Q1 results are consistent with the preliminary results that we announced on April 7th, we'll briefly review the highlights for the quarter and then spend some time discussing a few cost-saving measures that we undertook this past week. As a reminder, non-GAAP financial measures are reconciled to GAAP in the table at the end of today's press release. Non-GAAP revenue for the first quarter was \$65.7 million, an 8% increase over the prior year. Billings for the first quarter were \$69.1 million, a 4% increase over a year. Non-GAAP net income for Q1 was \$5 million or \$0.07 per fully diluted share.

The shortfall relative to our guidance issued on February 4th was largely related to the two issues that we discussed on April 7th. First, our North America commercial business was significantly impacted by a combination of macroeconomic headwinds causing customers to delay purchasing decisions. Second, our U.S. Federal team fell short of their goal due to contracting delays and budgeting issues related to the continuing resolution that the government was operating under at that time. In the last six business days of the quarter, approximately \$11 million of revenue from our commit line was pushed out of Q1. Importantly, our EMEA and Asia Pac teams experienced very solid performance, delivering at or close to their target.

In Q1, international billings were 41% of total billings. Domestic billings, excluding the U.S. federal government were 42% of total billing, and the U.S. federal government represented 17% of our total billing. In the first quarter, billings for our gateway security products were 86% of total billing and billings for identity and access products were 14% of total billing. In the quarter, we closed five individual transactions greater than \$1 million and an additional 110 deals over \$100,000. Deferred revenue increased \$6.2 million or 4% sequentially. At end of March, the total deferred revenue balance was \$174.4 million. As expected, non-GAAP gross margin was 75% of revenue. Non-GAAP operating income for the quarter was 10% of revenue. In Q1, we generated a \$13.1 million in cash from operations. The company's cash and restricted cash balance was \$23.7 million on March 31st.

Before I turn to Q2 guidance, I would like to discuss the cost-saving measures we undertook this past week. These measures included the elimination of 75 open positions that we had been planning to fill, the elimination of 75 current positions, additional reductions in non employee-related expenses from plan levels by \$500,000 per quarter, and additionally we've reduced our planned capital spending by approximately \$5 million for the balance of the year. A few other items to stress. We are maintaining an appropriate headcount in investment and engineering in order to continue fostering innovation, and the steps taken should reduce our forecasted expenses for 2008 by approximately \$10 million, which equates to an annual amount of approximately \$14 million to \$15 million.

Now I would like to turn to our outlook guidance, which is based on current expectations. All of these statements are forward looking and actual results could differ materially. For the second quarter 2008, we expect billings to be up slightly from Q1. Non-GAAP revenue is expected to be in the range of \$63 million to \$67 million. Non-GAAP gross margin is anticipated to be approximately 73 to 75% of non-GAAP revenue. Non-GAAP operating expenses are expected to be in the range of \$42 million to \$43 million. Fully diluted weighted average share count is expected to be approximately 75 million shares. Non-GAAP tax expense, which is also approximate, our actual cash outlay for taxes is expected to be approximately \$300,000 to \$500,000.

Interest and other expense are expected to be approximately \$900,000, and Q2 non-GAAP earnings per share is expected to be approximately \$0.04 to \$0.07 per fully diluted share. We again expect the breakdown of our product lines in Q2 to be approximately 90% for enterprise gateway and approximately 10% for identity and access management. As in prior years, we expect to see a sequential decrease in our Q2 cash generation due to normal seasonality. In Q2, cash generated from operations is expected to be approximately \$3 million to \$4 million. And consistent with normal seasonality, we would expect Q3 cash generation from operation to increase to approximately \$6 million to \$8 million. We expect Federal billings for Q2 to account for 15 to 20% of total billings.

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

And before I turn the call over to Dan, I would like to point out that we're suspending full year '08 and '09 guidance. Given the uncertain macroeconomic guidance and the amount of deal slippage we experienced in Q1, we believe it's prudent to only provide Q1 guidance at this time. I'd like to turn the call over to Dan.

Dan Ryan - *Secure Computing Corporation - CEO*

Thank you, Tim, and good afternoon. We are disappointed with our Q1 results and are taking aggressive actions to improve our future performance. This includes restructuring described by Tim and the implementation of a growth plan that I will briefly describe now. Over the last several months, the senior management team has been developing a strategy that will allow us to better capitalize on the market opportunities before us and provide stronger top and bottom line growth. Our board of directors has endorsed this plan and we're now aggressively executing on it.

While there's certainly excellent growth opportunities for each of our product lines, I'm a big believer in focus. Our increased focus will take two forms. First, we will commit substantially more of our resources to the areas of our business where we believe we can be the clear market leader. And second, we'll narrow the scope on our remaining products to the market segments where we have proven success and an opportunity for segment leadership. Regarding the former, our simple objective is to become the clear leader in secure web gateway market over the next 18 months and to remain a leader in the e-mail gateway market. The secure web gateway is a lucrative golden opportunity, and we are already in the strong position there. According to Gardner, there's only a 10 to 15% penetration of these solutions in the enterprise and 20 to 25% annual growth is anticipated.

Hosted web security, while smaller today than appliance base, is expected to grow at 36% annually according to IDC. We plan to address the web gateway market with flexible hybrid delivery model and that means appliance based virtualized and hosted or in the cloud offerings. In the coming weeks, we will launch a hosted web security service to complement our already successful appliance based offerings as well as our recently announced virtual offerings.

The new SAS, or software to service offering, leverages our web gateway technology as well as the worldwide data center infrastructure that exists for TrustedSource today. We're excited about both our current situation, as this is our most successful growth area, and the ability to accelerate this area based on an incremental investment combined with the high growth opportunity in the market. We remain a leader in the secure mail gateway market as well, which is another attractive growth area and one that has substantial synergies with web security. Similarly, we plan to offer flexible delivery models to our customers there.

In summary, our long-term strategy for web and mail security is to allow our customers to purchase market-leading security services and deploy them across different platforms to mix and match any configuration. This will deliver service portability, common policy in reporting, and unified pricing across all delivery models. Next, with respect to narrowing our scope on the remaining products, we have an excellent franchise in secure firewall or Sidewinder, the industry's leading application firewall. Our success in government financial services and high assurance networks in regulated and other industries continues to be strong. We protect some of the world's most critical networks and applications. If there's valuable data to be protected, we are a strong solution that should be considered.

Secure's firewall is also unique in that it's a software product that is readily virtualized and we will take advantage of that as well. Also, we offer the only application firewall that's fully integrated with the Reputation system, our TrustedSource system. Our emphasis going forward will be to aggressively attack and lead these key segments of the broader firewall market. Similarly, with SafeWord, we have a great platform to build from with the reformulated users today. Our primary emphasis will continue to be remote access solutions that can be rapidly deployed in Microsoft centric environments.

To summarize, we've reduced our cost structure and we are substantially increasing our investment in the high-growth areas where we believe we have the opportunity for clear leadership. In the other areas, we're narrowing our scope, and we will continue to strengthen our team throughout the organization. To that end, I'm pleased to announce that Steve Kozachok will be joining Secure Computing next week as our new Senior Vice President, Secretary, and General Counsel. Steve comes to us from St. Jude Medical, where he served as Associate General Counselor for the last three years and was the primary lawyer responsible for business development efforts. Before that, Steve was a partner in the law firm of Dorsey & Whitney, where he was Lead Outside Merger and Acquisition Counsel to a Fortune 50 company. I speak for the entire management team in saying we remain highly optimistic about the future of Secure. Operator, we would now like to open the call to analysts' questions.

QUESTION AND ANSWER

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Operator

(OPERATOR INSTRUCTIONS) Our first question comes from Joel Fishbein with Lazard. Your line is open.

Joel Fishbein - Lazard Capital Markets - Analyst

A couple of questions. First can you give us more color on some of the product lines, Webwasher and Ironmail in particular, your secure web or secure mail, how they did in the quarter?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

We don't typically segment them out, but I will say that the -- our web gateway product line is certainly the highest growth area and is growing significantly higher than those market rate growths that we mentioned from Gardner's perspective, but beyond that we don't segment them.

Joel Fishbein - Lazard Capital Markets - Analyst

How about in terms of the competitive landscape there? Any better, any worse?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

I think that we're seeing the same competitors on the web gateway. I think that we feel we have an opening door to walk through or jump through, run through or whatever you say, that some of our competitors are quite busy with either digesting acquisitions or just embarking on them, a couple of our primary competitors. We're hoping that gives us a little bit more of an entry to really take that market. Our intention here is to dominate the web gateway market and that's really what you're going to see focus of this company be for the next year.

Joel Fishbein - Lazard Capital Markets - Analyst

The second question comes, regarding, Tim, you talked about last quarter. On the last call, about \$11 million got pushed from Q1. And even assuming you got half of that in Q1, you would have crushed the number. Why the lower guidance for Q2?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

Yes, we've never had that many deals or that amount of deals slip out of the end of a quarter as we discussed on the 7th. And although there are some results out there that did fine for Q1 and said they were fine for North America, there were certainly other data points where there is concerns about the North America economy, market, macroeconomic environment, et cetera. Given that we're looking at a phenomenon at the end of Q1 that we've never seen before and the overall macro environment in the Americas especially, we felt it to be prudent to be conservative as look into Q2.

Joel Fishbein - Lazard Capital Markets - Analyst

All right. I'll jump back into queue. Thanks.

Operator

Eric Martinuzzi, your line is open with Craig Hallum.

Eric Martinuzzi - Craig-Hallum Capital Group - Analyst

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Curious, given the guidance on the billings for Q2, I think up slightly from Q1 is the way you characterized it. That would imply a decline from a year ago. A year ago we had -- I think billings were \$70.7 million or so. So up slightly. Is that \$69.5 million or is that \$71 million? Could we be in a contracting mode here for the foreseeable future?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

I think we would say that we expect to be may be up slightly from prior year as well. But, again, when you look at the macro environment, we feel it prudent to look hard at the pipeline we have and feel comfortable with what's in that pipeline relative to expectations to close and guide appropriately. And that still means that there's basically two months to go on this quarter. There's a lot of work to get done.

Eric Martinuzzi - Craig-Hallum Capital Group - Analyst

One more if I might. One of the things you've done is looked at your cost structure. What about your business segments? Is that on the table? Could we see potential strategic diversification here where maybe we aren't in certain businesses in the future that we currently are in?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

I don't think we have any particular plans to announce there, but I would say in looking at our strategy, anything's on the table. We'll do anything that we think maximizes the shareholder value and our growth opportunity and whether that's acquisitions or doing what you suggested.

Eric Martinuzzi - Craig-Hallum Capital Group - Analyst

Thank you.

Operator

Rob Owens with Pacific Crest Securities, your line is open.

Rob Owens - Pacific Crest Securities - Analyst

Yes, good afternoon, everyone.

Dan Ryan - Secure Computing Corporation - CEO

Hi, Rob.

Rob Owens - Pacific Crest Securities - Analyst

Any type of update you can give us with regard to the lawsuit with Finjan, where you're at in that process?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

Where the status is -- the jury has entered a verdict against us. We won on one count on the trial. They won on two counts. There was a verdict entered against us, and we have filed motions relative to that, we were asking the judge to set that aside, reduce the damages, et cetera, et cetera. Of course, Finjan has also filed motion for an injunction. All of the typical motions that both sides would file. We expect the judge to rule on those motions in three to five months, so sometime maybe in Q2. It might slip into July/August. Can't readily predict that. I'm sure whoever comes out on the short end of the judge's ruling will file appeals to the appellate court and that will take one year to two years to play out. A lot of game to be played there yet. As we've stated before, we don't believe that's going to be a material item to the company when it eventually does get resolved. But it's probably at least 1.5 years plus time rame before it's finally all put to rest.

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Rob Owens - Pacific Crest Securities - Analyst

Along those lines, is that causing any disruption in the selling process? Customer adoption team, I guess?

Dan Ryan - Secure Computing Corporation - CEO

It's certainly been distracting to us as a company. I think obviously Finjan is putting this out in the market in front of a lot of prospective customers and trying to make something of that. I would say that -- I am aware of one substantial deal that we would directly relate to this. We're not aware of any other ones at this time. They may exist, but we're not aware of them, and there was one specific one we know. We should also -- I'm sure you've heard this before this infringement isn't about the broader Webwasher product line. It's about one element of that product line and we do have the ability to ship the product today without the alleged infringement if we chose to do that. We are obviously not choosing to do that, and we have a long ways to go in the fight. So I think -- another thing is we don't really see Finjan competing with us in many deals. The [Fillmore], the Bluecoats and WebCensus we're seeing on the Webwasher side. But I would say it hasn't been a terrible business environment for us because of it. It has been some distraction to it and there is some small business impact.

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

It's kind of a nuisance on the side. It's there. We have to deal with it. We don't see them that much, but it is a bit nuisance. You couldn't say it's had zero impact. It's been a nuisance.

Rob Owens - Pacific Crest Securities - Analyst

Great, thanks.

Operator

Jonathan Ruykhaver with ThinkEquity, your line is open.

Jonathan Ruykhaver - ThinkEquity Partners - Analyst

Good afternoon. It looks like you incurred \$2 million in legal expenses related to Finjan. Is that the type of run rate we should expect in terms of cash expense in the next few quarters?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

No. So, yes, you're correct we did incur a fairly significant item in Q1 because of the trial, et cetera. But going forward, probably \$300,000 to \$400,000 a quarter for a couple quarters or two or three quarters has been built in. That's what we would expect to incur for the balance of the year.

Jonathan Ruykhaver - ThinkEquity Partners - Analyst

That's not included in the non-GAAP guidance you gave?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

It is included.

Jonathan Ruykhaver - ThinkEquity Partners - Analyst

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

It is. Okay.

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

It is included.

Jonathan Ruykhaver - ThinkEquity Partners - Analyst

In terms of the \$11 million deals that slipped out of March, would you characterize most of those as network security products?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

We looked at that and yes, probably more gateway security than I am, but in some respects fairly evenly spread out across all four product lines.

Jonathan Ruykhaver - ThinkEquity Partners - Analyst

So you even saw some pushed out of the web security side?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

Yes, and it wasn't necessary to any product line. It seemed to be more focused by geography because we didn't see the slippage in EMEA in any type of product line nor in Asia Pac, but we saw it in North America and a little bit in lap and North America especially, and it seemed to be across all product lines. But at the end of the day, as Dan stated in either one of his questions or prepared remarks, was we still are seeing as far as all of the product lines go, an IDC would probably back this up as well. Our best growth opportunity, and we're seeing it in our activity, is in the web gateway area.

Jonathan Ruykhaver - ThinkEquity Partners - Analyst

Right. And I guess just going back to the network gateway marketplace. Is there a contraction that's occurring in that marketplace or is there heightened competition? I'm trying to get a sense of what is causing the problems in that particular market, because I think most of your gateway business is probably in the firewall marketplace.

Dan Ryan - Secure Computing Corporation - CEO

I don't think -- we have three gateway products: mail, web and firewall. I would say, as Tim said, there's some contraction in each. I don't think we're seeing any particular fallback in our network gateway business. We actually had a nice growth in that business over the past year. I think that the -- it doesn't have the kind of growth we're seeing in web gateway, but I don't think we've seen a particular fallback. We focus in on we have a very good position, I don't know if you call it a niche market or a sub segment of these high assurance network and we do a lot in government and financial services. And there's a lot of initiatives that are supporting whatever downturn there is economically when you have [PCI DFF] initiatives and this critical infrastructure initiatives are going on right now. We're in a lot of those deals. I wouldn't say that there was a pretty good fallout in our network gateway any more than any other --

Jonathan Ruykhaver - ThinkEquity Partners - Analyst

Year-over-year looking at the billings growth being flat year-over-year for the most part and you're saying the web gateway business is growing and mail is probably doing okay. It would have to be either the authentication or the firewall business that's been showing accelerated growth.

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Maybe another way to think about it is when the markets -- we perceive the markets to still be strong, it's just that they seem to be a little bit pressured right now. But we don't perceive it to be in the market. We perceive it more in the macroeconomic environment. Products are not going away -- they're getting pushed out. People are not saying they're not important or they're not going to do it. They're saying I need to get another signature or need to go back through CapEx committee or it's going to take us longer to get approved. What we're seeing is more of a macro pressure from the environment than a specific segment of the market that's kind of backing up.

Jonathan Ruykhaver - ThinkEquity Partners - Analyst

Okay. So is it safe to assume that based the revenue guidance for June, you're being pretty conservative still as it relates to closure rates, sales cycles, continue to deteriorate?

Dan Ryan - Secure Computing Corporation - CEO

That would be the way to think about it.

Jonathan Ruykhaver - ThinkEquity Partners - Analyst

All right, guys. Thanks.

Operator

Fred Ziegel with Soleil Securities, your line is open.

Dan Ryan - Secure Computing Corporation - CEO

Hey, Fred.

Fred Ziegel - Soleil Securities - Analyst

Let me ask a couple of things. First, on the bigger deals, I would presume they are generally multi-product in terms of people looking at doing a couple of different things?

Dan Ryan - Secure Computing Corporation - CEO

Probably more often they're not, actually, Fred. I would say many of the big deals tend to be single product, kind of enterprise rollout or enterprise deployment. We do have multi-product deals all the time, but I wouldn't characterize -- if you went through our biggest deals, they're more likely to be one product than they are to be three.

Fred Ziegel - Soleil Securities - Analyst

Okay.

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

I agree and what that actually provides us is the opportunity to cross sell which we're definitely seeing an uptick in.

Fred Ziegel - Soleil Securities - Analyst

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

But if we're going to defocus some areas of the business, does that opportunity go away?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

No, because I think what maybe -- paraphrase Dan's comments, it is focus in on the areas where each product is the strongest. So web and mail happen to be strong in broad areas and we can look to be market leaders there in broad areas. Whereas secure firewall, secure IM, they are potentially a little bit more focused or have the opportunity to be leaders in a little bit more focused area. And that's where we will have the most success cross selling also. It's focusing in where we're the strongest.

Dan Ryan - Secure Computing Corporation - CEO

If we have an account that's a big Webwasher account and they're looking for firewalls, we're not going to tell the salesperson not to introduce Sidewinder to the account because it's not in one of the key verticals. In reality, we'll have more cross selling in the two or three verticals for firewall than we would in the general world.

Fred Ziegel - Soleil Securities - Analyst

The 75 person headcount reduction -- how is that spread out across the various disciplines?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

We tried very hard to impact sales generation the least amount as possible, and we tried also to impact our development team probably second least amount possible. So what I'll call the service organizations within the company, legal, HR, marketing -- we tried also to limit the impact to marketing. That probably was third in line. But then the service organizations, the balance of marketing, legal, HR, finance, operations, IT, et cetera -- those groups really stepped up and said we're going to try to cut our costs as aggressively as possible because we want to maintain our investment in innovation and the road maps we're on and want to maintain the lead generation pipeline generation machine.

Dan Ryan - Secure Computing Corporation - CEO

Hopefully it's clear also from the discussion that we not only took that money out of the company that Tim described. We added specifically a substantial amount of money back to the web gateway development and go to market areas. So that's all built into the numbers that we gave you. So the actual cut was probably more substantial when you consider that addback.

Fred Ziegel - Soleil Securities - Analyst

Okay. All right, thanks.

Operator

Josh Jabs with Roth Capital, your line is open.

Josh Jabs - Roth Capital Partners - Analyst

Good afternoon.

Dan Ryan - Secure Computing Corporation - CEO

Hey, Josh.

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Josh Jabs - Roth Capital Partners - Analyst

On the previous call, you talked about the government sector, the Federal sector, and some of the issues that you had seen in Q1. How is that looking for Q2 and Q3?

Dan Ryan - Secure Computing Corporation - CEO

I would say we're cautiously optimistic about the U.S. federal government plan right now. Obviously we're fool me once or fool me once, right? But we're being cautious and I think we're seeing a strong opportunity there, a good comeback.

Josh Jabs - Roth Capital Partners - Analyst

And then, going back to this product diversification or consolidation or however this plays out. You mentioned the area of focus. At the same time, it seems like the market has been looking for more consolidated offerings. Specifically, how do you pull back in one area such as UTM, but continue to invest the others and does that mean more of a downmarket shift with the service's offerings?

Dan Ryan - Secure Computing Corporation - CEO

I think when you talk about the combination, the natural synergy is between web and mail. There's a much more natural synergy in selling those products together. And that is a consolidated offering. If you look at what we're doing, we're trying to come up with a set of services, web and mail-based services, that we don't care which ones you pick and how you want it delivered, whether it's in a box in the cloud. That is very synergistic, more so than with the firewall, with the firewall business I think. I would we're not trying to necessarily narrow our product breadth. However, we do want to be known for something and secure computing in the broader sense really hasn't been known for something. And our objective here is we want to take leadership in a market. That'll accelerate our channel and accelerate our customer acquisition. And then we can bring all of our other products into it as well.

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

I would submit to you, Josh, I think we're potentially a step or two or three ahead of our competitors in consolidation. We already consolidate at the web gateway services such as FSL, SML or anti-virus, web filtering, et cetera. We have the same type of consolidated services at the mail gateway with DLP encryption, AV, TrustedSource reputation. We have trusted reputation-based technology at the web as well. And look at our set of services at the enterprise gateway. I think Secure has actually been a leader in consolidating services at appropriate areas or appropriate spots in the network. Now what we're saying is we're going to take those spots and really focus in on trying to capitalize on our leadership there.

Dan Ryan - Secure Computing Corporation - CEO

One more example -- Tim brought up some good ones -- that the mail and web gateway, there's a lot of discussions in the market today about daily prevention or protection DLP. A lot of companies that we partner with on a regular basis in our web gateway solution. With these services, we have between web and mail, the vast majority of the deal [promised] in motion between those protocols, web and mail. One of the thing we want to do is provide DLP services with policy across them. We're going to continue consolidate, for in motion date. We're not trying to replace Vontu anybody on desktop-type applications, but the 80/20 rule is if you can stop the majority of it there, that's another great service we can consolidate.

Josh Jabs - Roth Capital Partners - Analyst

Moving to the service -- on the services side. Will that put you into competition with any of your service provider customers?

Dan Ryan - Secure Computing Corporation - CEO

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Not that we're aware of. We have some MSP partners that provide services. In fact, we would see an opportunity to actually license our services through other partners that could actually sell those services. We have no issue private labeling some of these hosted security services, if that makes sense.

Josh Jabs - Roth Capital Partners - Analyst

And then specifically on the OEM side with some of your services. I know you've expanded that quite a bit here this spring, but can you just give us some color on how that's going?

Dan Ryan - Secure Computing Corporation - CEO

Could you repeat that?

Josh Jabs - Roth Capital Partners - Analyst

The OEM with the partnerships specifically for TrustedSource?

Dan Ryan - Secure Computing Corporation - CEO

We continue to go down that path. I think we have several partnerships. I would say our most active partnerships are less around TrustedSource and more around virtualization and also working with Riverbed in some joint solutions. I think that the TrustedSource alliance we have had out there -- we continue to market that and to sell that and we're active there. I don't think that's a big revenue opportunity for us in the near term.

Josh Jabs - Roth Capital Partners - Analyst

Okay.

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

I think in a broad sense, we believe that -- and I think that quite a bit of the market or IT pundits would agree that eventually reputation-based technology is going to be a clear driver or gating factor for activity on the web, and TrustedSource is a leader there. It's best for us to continue the broad capture of data such that we can maintain TrustedSource as the true leader in that reputation based arena.

Dan Ryan - Secure Computing Corporation - CEO

That's another good point where we see synergy and consolidation between web and mail. We have TrustedSource reputation information now includes web reputation, malware, again mail reputation as we always have. And as we get into the cloud and all of a sudden have thousands more points of reference and data collection, because of our customers are going through the service. We just get that much more visibility on the data that's out there that we can correlate.

Josh Jabs - Roth Capital Partners - Analyst

Last question. A little bit of the shift in focus here, and the cost reductions cause a change in the comp structure that you recently introduced for your sales team?

Dan Ryan - Secure Computing Corporation - CEO

No, it will not. The comp structure with the emphasis on new business development and cross selling remains intact.

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Josh Jabs - Roth Capital Partners - Analyst

Okay. Great, thanks.

Dan Ryan - Secure Computing Corporation - CEO

It's definitely having an impact.

Operator

Sarah Friar with Goldman Sachs, your line is open.

Fred Green - Goldman Sachs - Analyst

Hey, this is Fred [Green] for Sarah. You're taking a pause in paying down your debt right now. How long do you expect before you resume paying it down and is there a certain amount of cash you're looking to keep on your books going forward?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

Yes, we have taken a pause, Fred, and the big reason we took a pause is because of the macroeconomic environment. And again, we just saw this macro environment and said maybe it would be better to put that cash on the balance sheet. I think -- although we have not determined an exact level of what we want on a balance sheet before we start paying again, I think somewhere between \$25 million and \$50 million. And that will be a discussion we have with the board on an ongoing basis. And then I think once we build it up to a certain level, we'll consider paying down more or maybe we'll build it up to a certain point where we can pay down some big chunks at certain time levels. For the near future, we're going to be putting the money on the balance sheet for now.

Fred Green - Goldman Sachs - Analyst

Okay. Great, and do you have an update on sort of how long you think it will be until you have a workaround for the Finjan patents?

Dan Ryan - Secure Computing Corporation - CEO

I don't know that -- I'm not going to talk about a workaround. We have the ability immediately to ship a product without the piece of the product that is alleged to infringe. We don't agree it infringes, but if we were caused to, we could ship a product without that. It's one type of detection mechanism among many on the product, and we can ship without that.

Fred Green - Goldman Sachs - Analyst

Thanks a lot.

Operator

Joe Maxa with Dougherty and Company, your line is open.

Joe Maxa - Dougherty & Company - Analyst

Regarding your SafeWord and your narrowing your focus to the remote access solutions, does this mean you're effectively taking yourselves out of the larger consumer authentication opportunities?

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Dan Ryan - Secure Computing Corporation - CEO

I think when we say focused, we have some of the largest deployments in the world too. So it's a little bit of a dichotomy. But with SafeWord 2008 and really the successful no touch channel we've built around SafeWord and Microsoft deployments, we're going to continue to put a lot of the focus there. That's what is growing well for us. That's what has the best channel progress right now and that's the one that we think we have some uniqueness. Our product rolls out in that environment very easily, much more readily than most products, and this is where the marketing focus would be, I'd say. I guess we'll still continue to sell into accounts we're in. This is where we see a nice, steady predictable growth through a relatively low-touch channel.

Joe Maxa - Dougherty & Company - Analyst

Are you see any changes in the market that will keep you from more aggressively going after the hardware token side?

Dan Ryan - Secure Computing Corporation - CEO

We do the mobile [pass-type] electronic token which of course everybody's anticipated would be replacing tokens and that has not come to fruition. We still have a vast majority of the business goes with physical tokens, and we haven't seen a substantial change in our business, at least right now. We keep anticipating we'll move to other forums. We're very aware of that, but it hasn't happened yet.

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

What Dan just said is may be the key item to both questions you asked, Joe, and as much as we continue to look for consumer opportunities, or et cetera, the token market is not evolving that quickly. It seems like remote access tokens is still the leading solution and the market has not really embraced the next step or the next direction. So, what we want to do currently is try and capitalize on that and make the most of that. In the meantime, we will certainly be paying attention to where does that next path really show up. So that we can then jump into that. At present, tokens, remote access, business enterprise, is still the leading drivers in that part of the market.

Joe Maxa - Dougherty & Company - Analyst

Great, thanks a lot, guys.

Operator

Katherine Egbert with Jefferies, your line is open.

Katherine Egbert - Jefferies & Company - Analyst

Hi, I think before you answered the question about what positions you cut and you said it was mainly services. What planned positions did you eliminate?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

I'm sorry, Katherine, you must be on a mobile. You're cracking up. We did eliminate services and you said what?

Katherine Egbert - Jefferies & Company - Analyst

What planned positions?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Oh, planned positions. Planned positions was a little bit more across the board. We're not seeing quite the level of growth that we have been planning on, and the plan, of course, had been kind of not -- it's not a perfect peanut butter spread across the whole organization, but it was spread across the whole organization. So the planned position was a little bit more evenly spread across the board.

Katherine Egbert - Jefferies & Company - Analyst

Thanks.

Operator

Eric Suppiger with Signal Hill, your line is open.

Eric Suppiger - Signal Hill Group LLC - Analyst

Good afternoon.

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

Hey, Eric.

Eric Suppiger - Signal Hill Group LLC - Analyst

Did you give the headcount earlier?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

No, but I think post the actions we've took this week, we should be right around 900.

Eric Suppiger - Signal Hill Group LLC - Analyst

And I presume at the end of the quarter it was 975? So all of the cuts have been done at this point?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

Yes, substantially, yes.

Eric Suppiger - Signal Hill Group LLC - Analyst

Okay, can you give us a little feel -- I guess I'm trying to understand what parts of the firewall market you're going to be redirecting your focus away from?

Dan Ryan - Secure Computing Corporation - CEO

Well, I think I would say we don't feel that we are probably a strong competitor in the general network firewall space horizontally, right. That's not our strength. We are much more specialized in high-value data, high-value applications. And in many cases our firewalls are used behind other perimeter firewalls. So I think what we're saying is that our development effort is going to be to double down where we win today. And we do a fantastic job in federal government, in financial services, and utilities in other areas where we're protecting high value applications and data,

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

and I think it's easy for us to find ourselves competing with network firewalls. It's easy to get drawn into those fights against the big firewall players.

And I think we want to pick the fights where we can win and really go aggressively after those instead. We don't want to find ourselves in every network deal. We want to be in the deals where they're high value and high margin and we have a layer 7 orientation, an application layer orientation where we have a 3 out of 4 chance of winning, not a 3 out of 4 chance of losing.

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

To add on briefly, we're going to compete with the same people, if it's a layer 3 or 4 deal. If it's a perimeter network deal, as we compete with when it's a layer 7 deal. When it's in front of an Oracle server or application et cetera. We're certainly going to compete. But we have a much better chance to win when it's a layer 7 oriented-type of project and that's where we really want to make sure. You get into those high assurance networks. That's where we're going to get a higher win ratio. So we're going to make sure we're really focusing in and competing in as many of those as possible.

Dan Ryan - Secure Computing Corporation - CEO

The other thing we mentioned briefly that we're just embarking on, we announced this week some activities we're doing in virtualization. Our product is a software product, effectively running on a hardened black box, but this is very easily virtualized. We don't have a lot of semiconductor dependencies. So we have some unique capability where people need virtual firewall capabilities that many of the other competitors do not have, and depend on silicon and proprietary platforms.

Eric Suppiger - Signal Hill Group LLC - Analyst

Okay, and then can you help us a little bit in terms of measuring how your stronger-performing products are performing? Specifically, I'm talking about the web gateway and the mail security products. You're not breaking them out, so can you give us some way of gauging how your success in those areas is performing since that's arguably where the greatest investor interest would lie?

Dan Ryan - Secure Computing Corporation - CEO

We're not breaking them out now. We may chose to do that, however, in the future so there would be more clarity on that. I would just say what I did mention, is that Gardner has said the market rate is growing for web -- is the least penetrated at 15% with growth rates depending on whether it's appliance or wholesale somewhere between 20 and 36%. And I think that our recent history for Webwasher has been in excess of those growth rates. I would say mail is almost inextricably -- it can't be removed from web. I think it's becoming part of web, particularly related to the web 2.0 protection opportunity with our SWAT program. Mail and web are a hybrid solution now, and we're seeing those will emerging more and more together in our eyes with our solutions. We'll probably talk about these together. We probably won't even separate. If we do more segmentation, it probably won't be to separate web from mail. It might be to separate web and mail from network and access.

Eric Suppiger - Signal Hill Group LLC - Analyst

As a sales strategy, are you moving away from bundling the firewall with either the web or the mail and just selling them on a bundled basis more often?

Dan Ryan - Secure Computing Corporation - CEO

We still sell the firewall as the right solution to put in front of our other gateways. Obviously, we try and put as many of our products in as possible, but I think that -- that's a different procurement in many cases. So there's just more synergy with web and mail and I think from a cloud perspective, having a hosted offering, having the flexibility of having remote offices or home or internet cafe users going through the cloud and people at corporate going through the appliance. We see a more natural synergy between mail and web services.

Eric Suppiger - Signal Hill Group LLC - Analyst

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Last one, is there much cost associated with the infrastructure for the hosted service?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

Yes, there's cost, of course, in rolling it out. And hopefully there's going to be a lot of costs because it will be so successful that we'll need a lot of capital and pipes going in. But we do have, I believe seven data centers around the world today that support our TrustedSource environment, so we're quite familiar with this. It's not like we're a startup diving into this for the first time. So it really is layering on hardware and software infrastructure in those data centers and in some cases increasing the pipestone.

Dan Ryan - Secure Computing Corporation - CEO

We have that in our plan. That's in the budget that we described to you.

Eric Suppiger - Signal Hill Group LLC - Analyst

Very good. Thank you.

Operator

Thank you, our last question comes from Todd Raker with Deutsche Bank. Your line is open.

Todd Raker - Deutsche Bank - Analyst

Hey, guys, two questions for you, can you hear me?

Dan Ryan - Secure Computing Corporation - CEO

Yes.

Todd Raker - Deutsche Bank - Analyst

First, just looking at the balance sheet, it look like long-term deferred revenue kind of came down as a percentage here. Are you seeing shorter duration bookings and if so what's driving it, the economy?

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

Actually yes to both. Yes, we did see a reduction in the longer term, and yes, when it was specifically cited as to why that would happen, the economy, budget dollars, cash flow was the most often-cited reason.

Todd Raker - Deutsche Bank - Analyst

And if I step back, you guys are clearly cautious with the outlook given the experience you had, but if I look more generally across the security space, the results by and large have been relatively robust. And it doesn't look like some of the larger companies in this space are seeing the same type of macro headwinds that you guys are.

Tim Steinkopf - Secure Computing Corporation - SVP of Operations & CFO

May. 01. 2008 / 4:30PM ET, SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Well, what I would say is that there are certainly a few companies that have had some troubles, along with us. I would agree with you that there's been some that have not. The interesting thing for us is that if our government business had not run into troubles via the budgeting, et cetera, we would have hit our numbers. And therefore, we would have put up potentially exceeds numbers, maybe a little short on billings, but the rest of the numbers, revenue and earnings, et cetera, cash flow, would have all been at the high end, if not maybe even exceeded guidance. And it's interesting, in analyzing that situation, there's some people -- I'm not saying we're predicting this, but in analyzing the situation looking forward, there's at least some level of concern that the Q2 will be when the commercial markets really come home to roost. And I think you've seen that in the more conservative guidance headed into Q2. So some companies have made their Q1 numbers. They've got it conservatively for Q2. We would have been in that same boat if we hadn't had the double whammy of government as well. I think for us we're very much -- we are somewhat concentrating on government. We will also have that concentration in finance and banking, which of course they're suffering from macro factors as well. That would be our view of it.

Todd Raker - Deutsche Bank - Analyst

All right, thanks, guys, appreciate it.

Operator

I'll turn the call back over to Dan Ryan.

Dan Ryan - Secure Computing Corporation - CEO

Well, thank you for joining us and thanks for taking the time to ask the questions. Hopefully we answered them and look forward to updating you on our progress in three months. We remain optimistic on our business and hopefully we'll have something good to report in three months.

Operator

Thank you. This does conclude today's conference call. You may disconnect at this time.

Exhibit 5

Vital Security for Web TM 7.0

Service Pack 3



User Manual



Joint Trial Exhibit

JTX-14

Case No. 06-369 GMS

Vital Security for Web 7.0, Service Pack 3 User Manual

© Copyright 2004 by Finjan Software Inc., and/or its subsidiaries

All rights reserved. All text and figures included in this publication are the exclusive property of Finjan Software, and may not be copied, reproduced, or used in any way without the express permission in writing from Finjan Software. Information in this document is subject to change without notice and does not present a commitment on the part of Finjan Software.

The Finjan Software products described in this document are protected by U.S. Patent No. 6092194, 6167520, 6480962, 6209103, 6298446, 6353892, and 6804780 may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, and Vital Security are trademarks or registered trademarks of Finjan Software, Inc., and/or its subsidiaries. All other registered and unregistered trademarks are the sole property of their respective owners.

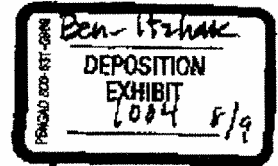
Finjan Software, Inc.	Finjan Software Ltd.
2025 Gateway Place	Shoham Building
Suite 180	1 Hamachshev Street, P. O. Box 8251
San Jose, CA 95110	Netanya South, Israel

Catalog number: VS4W_70_SP3_UM_RB

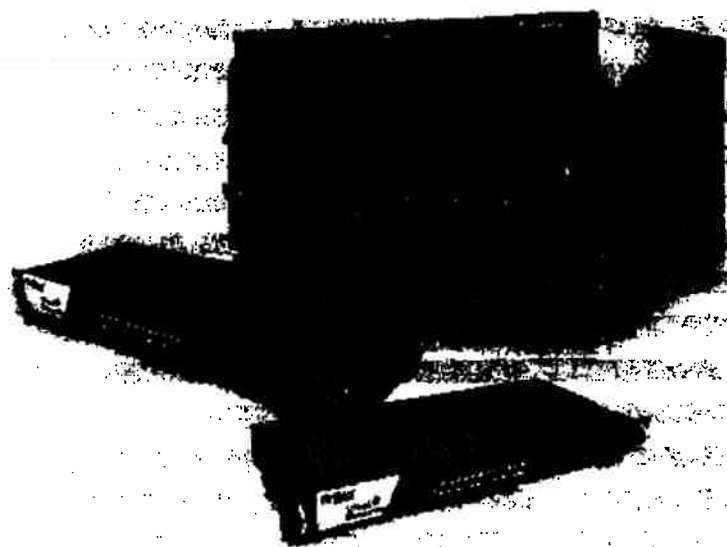
Exhibit 6



securing your web



Management Console Reference Guide



Vital Security™ Web Appliances
NG-1100/NG-5100/NG-8100

Defendant's Trial Ex.
DTX - 1070
Case No. 06-369 GMS

SC 11267

**Vital Security™ Web Appliances NG-1100/NG-5100/NG-8100 Management Console
Reference Guide**

© Copyright 1996 - 2006. Finjan Software Inc. and its affiliates and subsidiaries ("Finjan").
All rights reserved.

All text and figures included in this publication are the exclusive property of Finjan and are for your personal and non-commercial use. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, use or sell any part of its content in any way without the express permission in writing from Finjan. Information in this document is subject to change without notice and does not present a commitment or representation on the part of Finjan. The Finjan technology and/or products and/or software described and/or referenced in this material are protected by registered and/or pending patents including U.S. Patents No. 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892, 6804780, 6922693, 6944822, 6993662, 6965968 and 7058822 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Antidote and Window-of-Vulnerability are trademarks or registered trademarks of Finjan. Sophos is a registered trademark of Sophos plc. McAfee is a registered trademark of McAfee Inc. Kaspersky is a registered trademark of Kaspersky Lab. SurfControl is a registered trademark of SurfControl plc. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation. All other trademarks are the trademarks of their respective owners. Q3 2006.

For additional information, please visit www.finjan.com or contact one of our regional offices:

San Jose, USA

Toll Free: 1 888 FINJAN 8 (1 888 346 5268)
Tel: +1 408 452 9700
Email: salesna@finjan.com

New York, USA

Tel: +1 212 681 4410
Email: salesna@finjan.com

Asia Pacific

Tel: +972 (0)9 864 8200
Email: salesapac@finjan.com

United Kingdom

Tel: +44 (0)1252 511118
Email: salesuk@finjan.com

Germany

Tel: +49 (0)89 673 5970
Email: salescc@finjan.com

Israel

Tel: +972 (0)9 864 8200
Email: salesis@finjan.com

Catalog number: VSNG_MCRG
Email: support@finjan.com
Internet: www.finjan.com

Exhibit 7

Kobialka, Lisa

From: Kobialka, Lisa
Sent: Wednesday, February 27, 2008 10:36 AM
To: 'Holdreith, Jake M.'
Cc: Seidl, Christopher A.; Foster, Trevor J.; Schutz, Ronald J.; Moravetz, Amy; George, Sharon C.; Hannah, James; Andre, Paul; 'Rovner, Philip A.'
Subject: RE: Finjan v. Secure Computing Witness Notebooks

Jake,

Responses

Here are my responses to your questions.

1. We are also cutting down our depo designations. Please let us know when we can exchange the revised designations, so we can work through the counters, etc. and objections.
2. We will be dropping claims and will do so with prejudice if the parties agree there is no case and controversy in this litigation with respect to those claims. We will let you know which claims we are dropping. Also, can you confirm whether you will be dropping any claims and that we can reach the same agreement?
3. Mr. Jaeger will be in our rebuttal case.

Questions

1. Can you let me know who will be your corporate designee at trial? We will have Yuval Ben-Itzak.
2. Are you dropping DOE from your case against Finjan?
3. Wallach's opinion and testimony at deposition (p. 117) is that if Webwasher infringes, then Authenticode and Signed Java anticipate Finjan's patents. Since we are asserting that Webwasher infringes, that is his position. We want to confirm that you agree because if you do not, we will need to address this with the Court before trial starts.
4. Wallach asserted that he was not given access to Finjan's source code in his expert report. This is simply not true as we have several letters confirming that we made the source code for Mirage, Vital Security for Documents and Documents 1Box available.

Additional Responses to my initial email questions

With respect to my points from my email below, here are responses as best as we can via email. I would prefer to do this via phone and am willing to make myself available if you get back to me about when someone from your team is available to speak.

1. DTX 1057 is not a copy of German Exhibit 4 that was marked at the deposition based on what we have. DTX 1057 has different handwritten notes on it, even though it has the same bates numbers and has a cover page that it is German Exhibit 4. Our copy of German Exhibit 4 is not the same and we have the original transcript and exhibit. We want to understand where you got this copy of German Exhibit 4 because it is not the same as what we have.
2. Since you are not pursuing contributory infringement, we need to make the appropriate changes to the jury instructions and verdict form. We need to discuss this right away.
4. The Court specifically told us to meet and confer regarding the expert reports. Stating that what was said at the Pretrial Conference and at deposition does not cover it. We request a discussion about this, so we can confirm which position you are taking. We are asserting that Webwasher infringes. Therefore, Wallach's position cannot be that list means linked list because he took the position that linked list only came into play if Webwasher does not infringe.
6. In Wallach's report and deposition, he stated that he does not have an opinion regarding the ordinary meaning of "addressed to a client." We are confirming that he will not be testifying about this term's meaning.

5/16/2008

7. Are you confirming that for 112, Wallach is limited to paragraph 94 of Wallach's report? That was all that was identified at the Pretrial Conference. Furthermore, paragraph 94 does not cover all aspects of 112, which you currently have included in the jury instructions and special verdict form. We need to meet and confer about this as well too.

8. It appears from Wallach's rebuttal report that he is reiterating a version of defendants' original claim construction that was rejected by the Court. So we need to meet and confer that he is not using a substantially similar claim construction that has been rejected. This is something that we need to discuss.

Please let us know when you are available to discuss. We need to resolve them today, otherwise we need to notify the Court.

Very truly yours,

Lisa Kobialka

King & Spalding LLP
1000 Bridge Parkway, Suite 100
Redwood Shores, CA 94065
Ph: (650) 590-0720
Fax: (650) 590-1900

From: Holdreith, Jake M. [mailto:JMHoldreith@rkmc.com]

Sent: Wednesday, February 27, 2008 5:51 AM

To: Kobialka, Lisa

Cc: Seidl, Christopher A.; Foster, Trevor J.; Schutz, Ronald J.; Moravetz, Amy; George, Sharon C.

Subject: RE: Finjan v. Secure Computing Witness Notebooks

>>>> Please read the confidentiality statement below <<<<

Lisa, see my comments and questions below in response to your questions 1 -8. This may focus our meet and confer. Please give me your response and then we can set up a call.

We do have some questions for you:

1. We need to resolve objections to the designated deposition testimony as directed by Judge Sleet. We plan to cut down our designations and send them to you. Let us know if you will be cutting your designations down. At that point, perhaps we could each narrow our objections to those we would otherwise press at trial and see if we can then come to agreement.

2. You said you may be dropping claims. Please let us know which claims you intend to drop and whether you agree to drop them with prejudice. As I wrote before, if you are dropping them with prejudice we will likely agree not to pursue invalidity of the claims you drop.

3. You listed Mr. Jaeger as a witness you will call in your "case in chief." I don't believe Mr. Jaeger has disclosed any opinion you could offer in your case in chief proper, but only in your answering case. I expect you are calling Mr. Jaeger only in answer to our case and after we put our witnesses on, and not in your case in chief proper. Please advise.

5/16/2008

My responses/questions to your eight numbered questions are set forth following each of your eight points below.

Jake Holdreith

-----Original Message-----

From: Kobialka, Lisa [<mailto:lkobialka@KSLAW.com>]

Sent: Tuesday, February 26, 2008 1:01 PM

To: Seidl, Christopher A.

Cc: Foster, Trevor J.; Terry, Dannah G.; Schutz, Ronald J.; Moravetz, Amy; provner@potteranderson.com; Holdreith, Jake M.

Subject: RE: Finjan v. Secure Computing Witness Notebooks

Importance: High

When will you be available to discuss the other points? I would like to do it today or tomorrow if possible because it effects potentially some additional pretrial issues. Pursuant to the Pretrial Conference, we need to be sure there are no additional issues we need to raise with the Court prior to trial. Please let me know.

Very truly yours,

Lisa Kobialka

King & Spalding LLP

1000 Bridge Parkway, Suite 100

Redwood Shores, CA 94065

Ph: (650) 590-0720

Fax: (650) 590-1900

-----Original Message-----

From: Seidl, Christopher A. [<mailto:CASeidl@rkmc.com>]

Sent: Monday, February 25, 2008 7:30 PM

To: Kobialka, Lisa

Cc: Foster, Trevor J.; Terry, Dannah G.; Schutz, Ronald J.; Moravetz, Amy; provner@potteranderson.com; Holdreith, Jake M.

Subject: RE: Finjan v. Secure Computing Witness Notebooks

>>>> Please read the confidentiality statement below <<<<

Lisa,

Regarding number 3 below, we plan on sending you a proposed prosecution history estoppel instruction tomorrow.

Chris

-----Original Message-----

From: Kobialka, Lisa [<mailto:lkobialka@KSLAW.com>]

Sent: Monday, February 25, 2008 2:17 PM

To: Holdreith, Jake M.

Cc: Seidl, Christopher A.; Foster, Trevor J.; Terry, Dannah G.; Schutz, Ronald J.; Moravetz, Amy; provner@potteranderson.com

5/16/2008

Subject: RE: Finjan v. Secure Computing Witness Notebooks

Thanks. We will give you a call at 1 pm PST.

A few of the issues that we want to cover includes the following:

1) Where did you get DTX 1057 from? The version you sent us is not a copy of German Exhibit 4, even though the first page has German Exhibit

4 on it.

I don't understand your question. It is the exhibit marked at Alme's deposition. That is what is in our set as far as I know. What bates numbers are on the document you are looking at?

See Alme Depo 36:22-37:2: (Exhibit 4 marked.)

MR. HANNAH: For the record, Exhibit 4 bears Bates number SC 03430 through SC 03467. That is a presentation entitled "Webwasher Proactive Scanning." It is a Secure Computing presentation, and it has "Webwasher" on the cover."

2) Whether you are pursuing contributory infringement at trial.

We are not pursuing contributory infringement.

3) Whether you plan to send a prosecution history estoppel instruction and when.

You should have it today.

4) Which definition of list is being used, in light of the representations at the Pretrial Conference.

I don't know how to clarify this further than the discussion at the pretrial conference. You know what your position will be. Our position is as stated in Dan Wallach's report and at his deposition.

5) Whether you intend to include priority dates as part of your trial presentation.

I think that is likely, but unless you are planning to make an issue of it, I don't expect it is of major importance. My understanding is that you do not dispute that all of the prior art on the exhibit list is prior to your earliest priority date.

6) Whether Wallach is going to stay within his report and deposition testimony regarding the "addressed to a client" element.

I don't understand your question. What is your concern?

7) Confirming that Wallach is not providing an opinion regarding 112.

Wallach is providing the opinions in his report and his deposition. As discussed at the pretrial conference, he is not testifying as to the ultimate conclusion under section 112, nor as to what the legal standard is. He is testifying as to underlying factual conclusions and technical opinions that are relevant to a 112 analysis.

8) Wallach's intended testimony regarding "a server to the client" in light of the Court's claim construction

order.

I don't understand your question. How do you think the Court's claim construction affects this portion of his opinion?

If you have some additional issues, please let me know.

Very truly yours,

Lisa Kobialka

King & Spalding LLP
1000 Bridge Parkway, Suite 100
Redwood Shores, CA 94065
Ph: (650) 590-0720
Fax: (650) 590-1900

-----Original Message-----

From: Holdreith, Jake M. [mailto:JMHoldreith@rkmc.com]

Sent: Monday, February 25, 2008 9:27 AM

To: Kobialka, Lisa

Cc: Seidl, Christopher A.; Foster, Trevor J.; Terry, Dannah G.; Schutz, Ronald J.; Moravetz, Amy; provner@potteranderson.com

Subject: RE: Finjan v. Secure Computing Witness Notebooks

>>>> Please read the confidentiality statement below <<<<
I'm available today until about 4:30 Central. Let me know what time works.

-----Original Message-----

From: Kobialka, Lisa [mailto:lkobialka@KSLAW.com]

Sent: Sunday, February 24, 2008 6:42 PM

To: Holdreith, Jake M.

Cc: Seidl, Christopher A.; Foster, Trevor J.; Terry, Dannah G.; Schutz, Ronald J.; Moravetz, Amy; provner@potteranderson.com

Subject: RE: Finjan v. Secure Computing Witness Notebooks

Jake,

Sorry I did not get back to you sooner. I was unable to make any of the proposed times you listed below. Do you have time to discuss this coming week? Also, what trial are you referencing below?

Also, we need to schedule a time to meet and confer pursuant to the Court's instructions at the pretrial conference regarding expert reports. We are available on Monday afternoon and Tuesday for such a call, after 9:30 am PST. Please let me know what times you or a member of your time are available for such a call.

Very truly yours,

Lisa Kobialka

5/16/2008

King & Spalding LLP
1000 Bridge Parkway, Suite 100
Redwood Shores, CA 94065
Ph: (650) 590-0720
Fax: (650) 590-1900

From: Holdreith, Jake M. [mailto:JMHoldreith@rkmc.com]
Sent: Friday, February 22, 2008 7:30 AM
To: Kobialka, Lisa
Cc: Seidl, Christopher A.; Foster, Trevor J.; Terry, Dannah G.; Schutz, Ronald J.; Moravetz, Amy
Subject: Finjan v. Secure Computing Witness Notebooks

>>>> Please read the confidentiality statement below <<<<
Lisa,

I would like to have a short call to discuss how we will comply with Judge Sleet's instruction for jury notebooks with copies of trial exhibits. We have been informed that Judge Sleet approved a stipulation in a case that was before him within the last several weeks under which an initial set of exhibits was provided to the jury, with supplementation by each side during trial.

It seems to me that the universe of exhibits that each party will reasonably need to keep on the exhibit lists, even after good faith attempts to pare the lists, is far too voluminous to be included in its entirety in jury notebooks, and the problem of unresolved objections would also arise.

I don't have a clear answer to how to meet the Judge's instruction in view of these practical problems, but I would like to discuss the following concepts:

1. I expect there will be a Finjan set of binders and a Secure Computing set of binders, with each of us responsible for producing and updating our own sets of binders for the jury. Perhaps there should also be a third set of binders for the joint exhibits. Alternatively, there could be one set of binders with all three categories, but that would impose an extra burden for coordination of production of the binders.

Perhaps we could provide three-hole punched copies of our respective exhibits.

2. We could reduce practical problems significantly if we can exclude voluminous exhibits (say documents over 5 pages) from the jury binders. Perhaps there could be exceptions for the patents-in-suit and a handful of other principal trial exhibits if necessary. I'm not sure yet how to deal with voluminous exhibits.

3. For the initial binders to be given to the jury at the start of trial, it seems to me logical that we would provide everything on the joint exhibit list, subject to any exception for voluminous documents.

It also seems logical that we would provide anything to be used in openings, and anything that we expect to introduce in our cases in chief. I think we will need to have a process to vet objections to this set before it is given to the jury.

4. Assuming we can not and will not provide the whole universe to the jury at the start of trial, we would need a process for updating the binders with anything that comes in during trial that is not already in the binders.

I am in a series of meetings today and over the weekend, so my schedule is a little crowded. If you are available, I could meet by phone today (Friday) between 9 and 10 Pacific time or tomorrow between 1 and 2 Pacific.

In addition, please advise whether for the claims you plan to drop you will drop them with prejudice. In that event, we would likely agree that validity of those claims need not be a part of the trial. We don't presently contemplate withdrawing any claims, but would agree to be bound by the same terms in the event we do drop any claims.

Jake Holdreith
Office phone: (612) 349-8483
Direct FAX : (612) 339-4181
E-mail address:jmholdreith@rkmc.com

2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis MN 55402-2015

www.rkmc.com

<http://www.rkmc.com> <<http://www.rkmc.com/>>

Information contained in this e-mail transmission may be privileged, confidential and covered by the Electronic Communications Privacy Act, 18 U.S.C. Sections 2510-2521.

If you are not the intended recipient, do not read, distribute, or reproduce this transmission.

If you have received this e-mail transmission in error, please notify us immediately of the error by return email and please delete the message from your system.

Pursuant to requirements related to practice before the U. S. Internal Revenue Service, any tax advice contained in this communication (including any attachments) is not intended to be used, and cannot be used, for purposes of (i) avoiding penalties imposed under the U. S.

Internal Revenue Code or (ii) promoting, marketing or recommending to another person any tax-related matter.

Thank you in advance for your cooperation.

Robins, Kaplan, Miller & Ciresi L.L.P.

<http://www.rkmc.com> <<http://www.rkmc.com/>>

Confidentiality Notice This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Confidentiality Notice This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Confidentiality Notice This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

Exhibit 8

Kastens, Kristopher

From: Kastens, Kris (Perkins Coie)
Sent: Friday, November 30, 2007 9:40 AM
To: 'Chris Seidl'
Cc: 'tjfooster@rkmc.com'; Hannah, James (Perkins Coie)
Subject: Finjan v Secure Computing FW: IronMail

Chris,

We have not yet received the information we requested regarding setting up the IronMail appliance. We have tried repeatedly to get the required information from you (see email chain below), but have not even received an update. Please provide us with the requested information or when we will be receiving this information.

Sincerely,
Kris

-----Original Message-----

From: Kastens, Kris (Perkins Coie)
Sent: Wednesday, November 21, 2007 5:17 PM
To: 'Chris Seidl'
Cc: Hannah, James (Perkins Coie)
Subject: FW: IronMail

Chris,

Could you update us on the status of the IronMail appliance log-in information? We would like to test to appliance as soon as possible. Please let us know when we can expect this to be resolved. The problems were outlined in the email James Hannah sent you 6 days ago (see below).

- Kris

-----Original Message-----

From: Hannah, James (Perkins Coie)
To: Christopher A. Seidl (caseidl@rkmc.com) <caseidl@rkmc.com>
Sent: Thu Nov 15 17:38:16 2007
Subject: IronMail

Chris,

We have made progress on setting up the IronMail appliance. We have now been able to provide the license that you forwarded into the appliance and have been able to see the user interface. However, now the appliance is requiring an administrator user name and password. The screen that we get says that the "Pre-Log On Cookie Has Expired." Can you give us the requisite log on information or is there anyone we can refer our question to in order to get the requisite log on information? Thanks.

James

James Hannah
Patent Attorney
Perkins Coie LLP
101 Jefferson Drive
Menlo Park, CA 94025
Phone: (650) 838-4307
Fax: (650) 838-4507
Email: jhannah@perkinscoie.com

Exhibit 9

ROBINS, KAPLAN, MILLER & CIRESI LLP

2800 LA SALLE PLAZA
800 LA SALLE AVENUE
MINNEAPOLIS, MN 55402 2015
TEL: 612-349-8500 FAX: 612-349-4181
www.rkmv.com

ATTORNEYS AT LAW

CHRISTOPHER A. SEIDL
612-349-8468

September 28, 2007

VIA FEDERAL EXPRESS

James Hannah, Esq.
Perkins Coie LLP
101 Jefferson Drive
Menlo Park, CA 94025-1114

Re: *Finjan Software, Ltd. v. Secure Computing Corporation, et al.*
Our File No.: 028487.0002

Dear James:

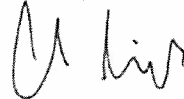
Enclosed please find a current version of the IronMail product. This product is being supplied pursuant to our agreement to allow you to inspect IronMail. Per our agreement, we offer this product for inspection for a period of 14 calendar days - please return the product and the entire contents of the box to me within 14 calendar days. The inspection of this product is subject to the Protective Order in this case and is deemed HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY.

Also enclosed is an Affidavit of Paul Judge.

Please let me know if you have any questions.

Regards,

ROBINS, KAPLAN, MILLER & CIRESI L.L.P.



Christopher A. Seidl

CAS/cjj
Enclosures

cc: Zhuanjia Gu (via Fax w/o enclosures)

FROM CIPHER TRUST

(FRI) SEP 28 2007 2:28/ST. 2:27/No. 6850897804 P 1

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

**FINJAN SOFTWARE, LTD., an Israel
corporation,**

Plaintiff-counterdefendants,

v.

**SECURE COMPUTING CORPORATION, a
Delaware corporation; CYBERGUARD
CORPORATION, a Delaware corporation,
WEBWASHER AG, a German corporation
and DOES 1 THROUGH 100,**

Defendants-counterclaimants.

Civil Action No. 06-369-GMS

AFFIDAVIT OF PAUL JUDGE

**STATE OF GEORGIA)
) ss.
COUNTY OF NORTH FULTON)**

I, Paul Judge, being first duly sworn on oath, depose and state that I have personal knowledge of the following facts:

1. My name is Paul Judge. I am over 18 years old. I have worked at Secure Computing Corporation since August 2006. I am currently Chief Technology Officer and Senior Vice President for Secure Computing. Prior to my employment at Secure Computing Corporation, I was the Chief Technology Officer at CipherTrust. As Chief Technology Officer at Secure Computing Corporation and formerly at CipherTrust, I have personal knowledge of the conception, design, structure, development, operation, features, and marketing of the IronMail product.

2. I understand that certain Secure Computing documents exist relating to the IronMail product that discuss "File Behavior Analysis." IronMail does not have, and has never had, the "File Behavior Analysis" feature referred to in these documents.

3. Any discussion of "File Behavior Analysis" in Secure Computing documents reflect a feature that was to be included in the IronMail product through an SDK agreement between CipherTrust (which was subsequently purchased by Secure Computing) and Finjan. The Finjan SDK was never implemented into IronMail for customer distribution. CipherTrust did build development versions of IronMail that included Finjan's SDK for testing and evaluation, but CipherTrust did so with Finjan's knowledge and consent and no development versions were distributed to customers or anyone else outside of CipherTrust or Secure Computing. During testing and evaluation of the development versions, CipherTrust was not satisfied with the Finjan SDK on Ironmail and, therefore, the IronMail/Finjan SDK project was put "on pause." Subsequently, CipherTrust was acquired by Secure Computing. In September 2006, after Secure Computing acquired CipherTrust, and while the IronMail/Finjan SDK project was still "on pause," Finjan terminated the agreement between CipherTrust and Finjan.

4. CipherTrust and Secure Computing attempted to remove all references to "File Behavior Analysis" in documents. The document identified by Finjan that references "File Behavior Analysis," which is numbered FIN000849-FIN000850 at the bottom, references an IronMail product that would have included Finjan's SDK if CipherTrust and/or Secure Computing had implemented it, but, as described above, neither CipherTrust nor Secure Computing ever did.

5. The IronMail product that Secure Computing is providing to Finjan for inspection in the above-entitled litigation is the IronMail S Class. This product is representative of Secure


FROM CIPHER TRUST

(FRI) SEP 28 2007 2:29/ST. 2:27/No. 6850897804 P 3

Computing's IronMail products. This product, the S Class, does not have, and has never had, the "File Behavior Analysis" feature discussed above, nor has any other IronMail product.

FURTHER, AFFIANT SAYETH NOT.

Dated: September 28, 2007


Paul Judge

Subscribed and sworn to before me
this 28th day of September, 2007.

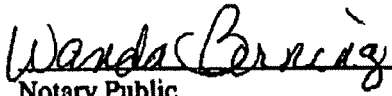

Notary Public
WANDA BERNING
Notary Public, Gwinnett, State of Georgia
My Commission Expires October 18, 2010



Exhibit 10

[illegible]

Testimonials	Patents	Management team	Milestones	Solutions
<p>"Secure Computing® has become a case study for illustrating how quality leadership, investment in employees, and superior product design with unwavering focus on custom service, has resulted in increased market share, revenues, and profitability."</p> <p>Jason Wright Industry Analyst Frost & Sullivan</p>	<p>Financial status</p> <p>Secure Computing is publicly traded on the Nasdaq national Market System under the symbol SCUR. Annual revenues (reclassified for discontinued operations of the Advanced Technology contract revenues):</p> <ul style="list-style-type: none"> • 2007 Fiscal Revenues: \$237.9M • 2006 Fiscal Revenues: \$176.7M • 2005 Fiscal Revenues: \$109.2M • 2004 Fiscal Revenues: \$93.40M • 2003 Fiscal Revenues: \$76.21M • 2002 Fiscal Revenues: \$61.96M • 2001 Fiscal Revenues: \$48.35M • 2000 Fiscal Revenues: \$34.64M • 1999 Fiscal Revenues: \$22.54M 			
	<p>Market opportunity</p> <p>Organizations today are expanding their businesses through the Internet daily. In this promising business environment, threats are also increasing right along with growth opportunities. Industry analyst IDC now expects the worldwide revenue for security hardware and software to be \$30 billion by 2009.</p> <p>Our customers need a secure infrastructure they can rely on. Accordingly, our commitment is to mitigate their risk exposure and protect their information assets from a multitude of threats, including identity theft, intruders, legal liability, security compromises, hackers, malicious software, and viruses.</p>			
	<p>Customers</p> <p>Secure Computing's customers operate some of the largest and most sensitive networks and applications in the world. They include the majority of the Dow Jones Global 50 Titans and numerous organizations in the Fortune 1000, as well as banking, financial services, healthcare, telecommunications, manufacturing, public utilities, schools, and federal and local governments. Secure Computing has close relationships with the largest agencies of the United States government, including multiple contracts for advanced security research. Overseas, our customers are concentrated primarily in Europe, Japan, China, the Pacific Rim, and Latin America.</p>			
	<p>Partners</p> <p>Our partnerships include a global network of OEMs, members of our Secure Alliance program, resellers, systems integrators, and companies that include our solutions in their product offerings. We offer our partners extensive</p>			

support through our PartnersFirst Program and Web site. All business except for a select group of key accounts are sold through our partners. These companies include, for example and among others: Alternative Technology, Blue Coat Systems, Cisco, Computer Associates, Comstor, Crossbeam, Dell, EDS, F5, Hewlett-Packard, McAfee, Microsoft, Network Appliance, NetOne Systems, Northrop Grumman, Novell, PGP Corporation, SafeNet, Sun PS, SAIC, Tech Data, Vertex Link, Voltage Security, Wavecrest Computing, Westcon, and Workshare.

Patents

Secure Computing is a leader in advanced research and development of network and systems security technology. Our team of distinguished researchers and scientists has achieved numerous breakthroughs in the security industry over the past 16 years. The company has been granted a total of 80 patents issued or pending in the United States. These patents cover systems architecture, cryptography, electronic mail filtering, and security control systems.

Management team

- Daniel Ryan — President, CEO, and COO
- Tim Steinkopf — Senior Vice President and Chief Financial Officer
- Mike Gallagher — Senior Vice President, Product Development and Support
- Glenn Cross — Senior Vice President, Worldwide Sales
- Atri Chatterjee — Senior Vice President, Marketing

Secure Computing and Enterprise Security Solutions

Secure Computing has long been regarded as the “gold standard” in enterprise firewall technology. Our award-winning products protect some of the most mission-critical networks and applications in the world. As these network environments have evolved with the growth of the Internet, we have added extensive capabilities in the areas of Web and messaging application security as well as identity and access management. Addressing the fundamental issues of application security has required a new approach which is embodied in our Enterprise Security portfolio solutions listed below.

TrustedSource™ - Global Intelligence to Protect Your Organization

TrustedSource technology is the most precise and comprehensive Internet host reputation system in the world, and a cornerstone of our solutions. TrustedSource uses data collected from over 7000 sensors worldwide to assign a reputation “score” to each sender encountered. This score is incorporated into Secure Computing products to enable them to quickly and accurately reject unwanted traffic.

Secure Web Solutions

inbound and outbound risks.

Secure Mail Product Portfolio

Secure Mail (IronMail)



Secure Mail (*IronMail*) delivers a centrally managed, integrated, best-of-breed messaging gateway security appliance for enterprises of all types and sizes.

Secure Mail Edge

Secure Mail Edge is a hardened appliance positioned at the perimeter of the mail system, applying TrustedSource technology to control email traffic at the network border.

Secure Mail Encryption

Secure Mail Encryption appliances deliver multiple encryption options with enough customizable flexibility for any security environment.

Secure Firewall Solutions

The definition of the "enterprise perimeter" has evolved significantly since the advent of the Web as mobile workforces, extranets, distributed applications, and an environment of highly sophisticated, blended threats has forced enterprises to deploy an array of security applications to provide services such as firewall, VPN, IDS/IPS, anti-virus, anti-spam and more.

As a pioneer in firewall technology and unified threat management, Secure Computing's application-layer products carry the highest possible Common Criteria certification and have never once been compromised in eleven years across thousands of deployments. Our ability to leverage TrustedSource technology to add real-time host profiling to our arsenal of security decision-making criteria makes Secure Computing's Secure Firewall Portfolio truly unique.

Secure Firewall product portfolio

Secure Firewall (Sidewinder)



Proven to be the most comprehensive security gateway appliance in the world, Secure Firewall security appliances consolidates all major Internet security functions into a single system to defend against known and unknown threats.

Secure Firewall CyberGuard TSP

Secure Computing's CyberGuard TSP appliances are designed to protect mid-sized to large enterprises against both known and zero-hour attacks, using a hybrid architecture that combines stateful packet filtering, seven layer inspection, and secure content policy enforcement.

Secure SnapGear

Secure SnapGear is a complete office-in-a-box Internet security appliance for small businesses, with wide area networking tools normally only available in enterprise-class devices.

Secure Firewall CommandCenter

Secure Firewall CommandCenter is Secure Computing's enterprise-class central management solution that enables you to implement security policies quickly, easily, and accurately across your entire security infrastructure (for both Secure Firewall (*Sidewinder* and *SnapGear* appliances)).

Secure SafeWord



Establishing the identity of users accessing corporate network resources, remotely and from the inside, as well as enforcing the policies governing the scope of these interactions, are critical functions of enterprise security. Secure Computing's Secure SafeWord two-factor authentication solutions allow you to protect VPNs, Citrix applications, Web applications, Webmail, and Outlook Web access.

Security Services

Our award winning support team offers hands-on installation, training services, and 24x7 support. www.securecomputing.com/goto/support

Milestones

- **March 2008**, Secure announces and launches new company-wide corporate and product branding
- **February 2008**, Webwasher Ranks #1 With a 99.9 Percent Catch Rate in a New Anti-Malware Study
- **January 2008**, New SafeWord 2008 Two-Factor Authentication Protects the Widest Range of Applications and Information
- **January 2008**, Secure Computing Named Worldwide Leader of the Web Security Appliances Market by Leading Market Research Firm

- **December 2007**, Secure Computing Achieves OPSEC Certification From Check Point
- **December 2007**, Sidewinder 7 Gateway Security Appliances Achieve EAL4 Common Criteria Certification Against U.S. Government Application-Level Firewall Protection Profile
- **November 2007**, New TrustedSource.org; Comprehensive Internet Reputation System Incorporates Malware Detection, Website Categorization and Spam Traffic Intelligence unveiled
- **October 2007**, Secure Computing Introduces CommandCenter for Significantly Improved Enterprise Management Capability
- **October 2007**, Secure Computing Unveils S.W.A.T.: (Secure Web 2.0 Anti-Threat) Initiative
- **September 2007**, Next Generation of Web Gateway Security Solution – Webwasher released
- **August 2007**, Secure Computing Positioned as "Top Player" in Radicati Group's Email Security Appliances Market Report
- **July 2007**, New Solution From Secure Computing -- MobilePass, Generates One-Time Passcodes on Users' Mobile Devices
- **June 2007**, Secure Computing Fortifies Industry-Leading URL Filtering Solution SmartFilter with TrustedSource Next-Gen Reputation System
- **June 2007**, Secure Computing Positioned in the Leader's Quadrant for Secure Web Gateway Magic Quadrant
- **June 2007**, Secure Computing's Web Gateway Anti-Malware Engine Beats 28 Competitors to Win Top Honors in Anti-Malware Roundup
- **May 2007**, Next Generation of SnapGear SMB Network Security Appliance with TrustedSource released
- **May 2007**, Secure Computing Launches Industry's First Self-Serve Domain Health Check
- **April 2007**, Awarded Three New Patents for Web and Messaging Gateway Security technologies
- **March 2007**, SC Magazine Bestows 'Best Buy' Honors on Secure Computing's IronMail
- **March 2007**, Secure Computing's Web Gateway Security Ranks #1 in Independent Office Documents Security Study
- **February 2007**, Sidewinder Wins SC Magazine Reader's Trust Award for Best Enterprise Firewall
- **January 2007**, Sidewinder 7.0 and Webwasher 6.5 releases announced
- **January 2007**, Latest version of market-leading reputation system TrustedSource released
- **December 2006**, Sidewinder G2 received Editor's Choice Award for functionality and security from Communications Week
- **December 2006**, Secure Computing honored with Best of 2006 awards for TSP 7300, SafeWord PremierAccess, and Webwasher
- **December 2006**, Secure Computing receives Reader Trust Finalist status from SC Magazine for Sidewinder G2, IronIM, and SmartFilter

- **December 2006**, Introduced the sleek, new carabiner-style Alpine token
- **November 2006**, Webwasher 6.0 released
- **October 2006**, Secure Computing positioned in the Leaders Quadrant for Gartner E-Mail Security Boundary 2006
- **October 2006**, Webwasher ranked the number 1 product for detecting the most malware by eWeek Magazine
- **October 2006**, Secure Computing holds Messaging Security Conference in Las Vegas
- **September 2006**, SnapGear awarded CRN Test Center's "Recommended" for Securing Wired and Wireless Access for SMEs
- **September 2006**, Secure Computing announces SafeWord SecureWire 50 IAM appliance for SMEs
- **August 2006**, Secure Computing closes acquisition of CipherTrust
- **August 2006**, Sidewinder G2 named Best MidMarket Product of the Year by CMP's VARBusiness Magazine
- **July 2006**, CyberGuard TSP achieves Common Criteria Certification using stringent DOD profile
- **July 2006**, Secure Computing announces intention to merge with CipherTrust, Leader in Messaging Security
- **June 2006**, Secure Computing named to FORTUNE Small Business Fastest-Growing Small Companies List
- **June 2006**, Secure Computing Positioned in Challengers Quadrant of Leading Analyst Firm's Magic Quadrant
- **June 2006**, Secure Computing Named to Business 2.0's 100 Fastest-Growing Technology Companies List
- **June 2006**, Announces Worldwide Channel Launch of Webwasher Secure Content Management Suite
- **May 2006**, IronMail named SC Magazine's Best Security Solution for Healthcare
- **May 2006**, Announces SafeWord PremierAccess 4.0
- **May 2006**, Sidewinder G2 Security Appliance Cryptographic Module for SecureOS Achieves FIPS 140-2 Validation
- **May 2006**, Secure Computing Honored with Reader Trust Awards from SC Magazine for Webwasher, SafeWord, SmartFilter
- **April 2006**, Extends TSP Portfolio to Support Unified Threat Management
- **April 2006**, Launches SafeWord SecureWire Identity and Access Management Appliance
- **March 2006**, Announces SnapGear Family of security appliances available to the Secure Computing worldwide channel
- **March 2006**, Secure Computing wins VARBusiness Magazine's 5-Star Rating 3 consecutive years

- **February 2006**, Information Security Magazine names IronMail 2006 Product of the Year
- **February 2006**, Announced Zero-hour Attack Protections technology inside Sidewinder G2
- **January 2006**, Acquires CyberGuard Corporation
- **November 2005**, Secure Computing reaches 1,000 Partner Milestone
- **September 2005**, Announces relationship with McAfee's line of SCM appliances to run SmartFilter technology
- **August 2005**, Celebrates Sidewinder G2 10-year flawless record of Zero compromises
- **August 2005**, Releases SmartFilter 4.1
- **June 2005**, Launches Sidewinder G2 Security Reporter
- **May 2005**, Sidewinder G2 first to achieve Common Criteria Certification using stringent DoD Application Firewall Medium Robustness Protection Profile
- **April 2005**, Secure Computing announces partnership with Sophos
- **March 2005**, Secure Computing wins VARBusiness Magazine's 5-Star Rating 2 consecutive years
- **February 2005**, SmartFilter wins SC Magazine Global Award
- **February 2005**, Announced 2005 new Sidewinder G2 lineup, including new SMB models
- **December 2004**, Sidewinder G2 named Product of the Year by Information Security Magazine
- **September 2004**, Secure Computing announces new version of SafeWord RemoteAccess 2.0
- **September 2004**, Launched Safeword PremierAccess 3.2
- **September 2004**, Launched SafeWord RemoteAccess, Cisco compatible
- **August 2004**, Sidewinder G2 Security Appliance receives EAL4+ Certification
- **June 2004**, Launched SmartFilter 4.0
- **January 2004**, Accelerated PartnersFirst Program by turning all but a select group of key accounts to channel partners
- **January 2004**, Announced Sidewinder G2 Security Appliance line
- **November 2003**, Announced SafeWord for Nortel Networks
- **October 2003**, Announced SafeWord for Check Point
- **October 2003**, Announced final acquisition of N2H2
- **August 2003**, SmartFilter receives OPSEC certification
- **July 2003**, Sidewinder G2 Firewall receives ICSA IPSec 1.1 certification
- **April 2003**, Sidewinder G2 Firewall achieves Common Criteria EAL4+ certification
- **April 2003**, Announced SafeWord for Citrix MetaFrame
- **February 2003**, Announced SmartFilter v3.2
- **January 2003**, Announced Sidewinder G2 Firewall and Sidewinder G2 Enterprise Manager
- **January 2003**, SmartFilter available on Cisco Routers

- **January 2003**, John McNulty named CEO of the year for Network Security by Frost & Sullivan
- **June 2002**, Unveiled next generation firewall plans
- **May 2002**, Announced SafeWord PremierAccess v3.1
- **April 2002**, Gauntlet awarded Common Criteria EAL4 level certification
- **February 2002**, Announced acquisition of Gauntlet firewall and VPN business
- **January 2002**, Announced Sidewinder Appliance
- **December 2001**, Announced SecureAlliance program
- **November 2001**, Sidewinder receives ICSA IPSec certification
- **October 2001**, Introduced SafeWord PremierAccess access control software for managing user authentication and authorization for e-Business applications
- **July 2001**, Sidewinder first firewall accepted into a Common Criteria Evaluation Assurance Level 4+
- **April 2001**, Introduced industry's first Embedded Firewall product
- **April 2001**, Announced \$100,000 e-Security Challenge
- **1999**, Sidewinder receives Firewall of the Year from Network Magazine
- **1995-1996**, Acquired technology for two market leading access control products – SafeWord® authentication, and SmartFilter® URL filtering
- **1995**, Announced Sidewinder challenge
- **1995**, Introduced the world's first truly secure proxy-based firewall, Sidewinder®
- **1995**, Initial Public Offering
- **1989**, Spun off as Secure Computing Corporation
- **1984**, Secure Computing started as the Secure Computing Technology Center division of Honeywell

Secure Computing is a global leader in Enterprise Gateway Security software solutions. Powered by our TrustedSource technology which provides real-time web and messaging reputation scoring, our award winning portfolio of email, Web, and application firewall security solutions provide anti-spam, anti-virus, anti-phishing, anti-malware, and anti-spyware prevention and protection to help ensure enterprise network security. Secure Computing's security software and network appliances also provide data leakage prevention, regulatory compliance, including robust auditing and reporting, strong authentication, and identity management.

Copyright © 2008 Secure Computing Corporation. All Rights Reserved.

[Home](#) | [Contact](#) | [Privacy Policy](#) | [Disclaimer](#) | [Sitemap](#)

[Access Control](#) | [Anti-malware](#) | [Anti-phishing](#) | [Anti-spam](#) | [Anti-spyware](#) | [Anti-virus](#) | [Application Firewall](#) | [Auditing & Reporting](#) | [Authentication](#) | [C/PA Compliance](#) | [Common Criteria](#) | [Content Filtering](#) | [Data Leakage](#) | [Email Security](#) | [Enterprise Gateway Security](#) | [Firewall](#) | [Global Intelligence](#) | [Identity Management](#) | [Internet Security](#) | [Intrusion Detection](#) | [Intrusion Prevention](#) | [Messaging Gateway Security](#) | [Network Gateway Security](#) | [Network Management](#) | [Network Security](#) | [Network security software](#) | [Online Banking](#) | [Password](#) | [PCI DSS](#) | [Radius Authentication](#) | [Regulations Compliance](#) | [Remote Access](#) | [Reputation Score](#) | [Reputation System](#) | [Security Appliance](#) | [Security Audit](#) | [Security Policy](#) | [Security Software](#) | [Spam Blocker](#) | [Spam Filter](#) | [Spam Prevention](#) | [Strong Authentication](#) | [Unified Threat Management](#) | [UTM Security](#) | [Virus Blocker](#) | [Virus Protection](#) | [Virus Signature](#) | [VPN](#) | [Web 2.0 Threats](#) | [Web Filtering](#) | [Web Gateway Security](#) | [Web Reputation](#) | [Web Security](#) | [Wireless Network Security](#)

© Secure Computing Corporation. All Rights Reserved. Secure Computing, SafeWord, Type Enforcement, MobilePass, SecureSupport, SecureOS, SnapGear and Strikeback are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. SecureWire, TrustedSource, SmartReporter, and SecurityReporter are trademarks of Secure Computing Corporation.